



No 1 P 0 9 9 1 U S (B)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2 0 0 1 年 2 月 2 3 日

出 願 番 号

Application Number:

特 願 2 0 0 1 - 0 4 8 9 1 6

出 願 人

Applicant(s):

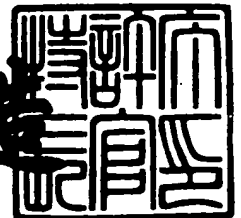
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2 0 0 1 年 5 月 3 0 日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2 0 0 1 - 3 0 4 7 3 4 7

【書類名】 特許願

【整理番号】 0100042207

【提出日】 平成13年 2月23日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 H04K 1/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 大嶋 拓哉

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 大塚 武

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 本城 哲

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 荒川 真志

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100095957

【弁理士】

【氏名又は名称】 亀谷 美明

【電話番号】 03-3226-6631

【先の出願に基づく優先権主張】

【出願番号】 特願2000-142307

【出願日】 平成12年 5月10日

【手数料の表示】

【予納台帳番号】 040224

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0012374

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカード、コンピュータプログラムおよび記憶媒体

【特許請求の範囲】

【請求項１】 価値情報が記憶されたＩＣカードと、前記ＩＣカードに対する情報入出力機能を備えたクライアント装置と、商品またはサービスを提供する店舗装置と、前記ＩＣカードと前記店舗装置間の決済を管理する決済管理装置と、前記クライアント装置と前記店舗装置と前記決済管理装置とを双方向通信可能に接続する通信系とから成る電子決済システムであって、

前記決済管理装置は、前記ＩＣカードで決済を行うための決済情報を、前記店舗装置からの決済要求情報に基づいて生成し、前記決済情報を前記決済管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、この暗号化された決済情報を前記クライアント装置に送信し、

前記クライアント装置は、前記決済管理装置から受信した前記決済情報を前記ＩＣカードに出力することを特徴とする、電子決済システム。

【請求項２】 前記店舗装置は、前記決済要求情報の正当性を示す第１署名を前記店舗装置の秘密鍵を用いて作成し、前記第１署名が付された前記決済要求情報を前記決済管理装置に送信し、

前記決済管理装置は、前記店舗装置から受信した前記第１署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項１記載の電子決済システム。

【請求項３】 前記第１署名が付された前記決済要求情報は、前記クライアント装置を介して前記決済管理装置に送信されることを特徴とする、請求項２記載の電子決済システム。

【請求項４】 前記決済管理装置は、前記第１署名付き決済情報の正当性を示す第２署名を前記決済管理装置の秘密鍵を用いて作成し、この第２署名が付され暗号化された前記決済情報を前記クライアント装置に送信し、

前記クライアント装置は、前記決済管理装置から受信した前記第２署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記決

済情報を前記 IC カードに出力することを特徴とする、請求項 2 記載の電子決済システム。

【請求項 5】 前記決済管理装置は、決済完了情報を生成し、この決済完了情報の正当性を示す第 3 署名を前記決済管理装置の秘密鍵を用いて生成し、前記決済情報を含むとともにこの第 3 署名が付された前記決済完了情報を前記店舗装置に送信し、

前記店舗装置は、前記決済管理装置から受信した前記第 3 署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項 1 記載の電子決済システム。

【請求項 6】 前記店舗装置は、前記第 3 署名が付された決済完了情報を受信し、前記店舗装置の秘密鍵を用いて第 4 署名付き決済完了受領情報を生成し、この第 4 署名付き決済完了受領情報を前記決済管理装置および前記クライアント装置に送信し、

前記決済管理装置および前記クライアント装置は、前記店舗装置から受信した前記第 4 署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項第 5 記載の電子決済システム。

【請求項 7】 前記店舗装置は、複数の下層店舗装置を含むモールとして構成されていることを特徴とする、請求項 1 記載の電子決済システム。

【請求項 8】 IC カードに記憶されている価値情報をクライアント装置を介して更新することが可能な決済管理装置において、

前記決済管理装置は、前記 IC カードの価値更新情報を前記決済管理装置と前記 IC カードとの間で共用される共通鍵を用いて暗号化し、この暗号化された価値更新情報を前記クライアント装置に送信し、

前記クライアント装置は、受信した前記価値更新情報を前記 IC カードに入力することを特徴とする、決済管理装置。

【請求項 9】 前記決済管理装置は、前記価値更新情報の正当性を示す第 5 署名を前記決済管理装置の秘密鍵を用いて生成し、前記第 5 署名が付された前記価値更新情報を前記クライアント装置に送信し、

前記クライアント装置は、前記決済管理装置から受信した前記第 5 署名の正当

性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記価値更新情報を前記ＩＣカードに入力することを特徴とする、請求項８記載の決済管理装置。

【請求項１０】 価値情報が記憶されたＩＣカードと商品またはサービスを提供する店舗装置との間の決済を管理する決済管理装置において、

前記ＩＣカードで決済を行うための決済情報を、前記店舗装置からの決済要求情報に基づいて生成する決済情報生成部と、

前記決済情報を前記決済管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化する決済情報暗号化部と、

この暗号化された決済情報を前記ＩＣカードに対する情報入出力機能を備えたクライアント装置を介して前記ＩＣカードに出力する決済情報出力部とを備えたことを特徴とする、決済管理装置。

【請求項１１】 前記店舗装置は、前記決済要求情報の正当性を示す第１署名を前記店舗装置の秘密鍵を用いて作成し、前記第１署名が付された前記決済要求情報を前記決済管理装置に送信し、

前記決済管理装置は、前記店舗装置から受信した前記第１署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項１０記載の決済管理装置。

【請求項１２】 前記決済管理装置は、前記第１署名付き決済情報の正当性を示す第２署名を前記決済管理装置の秘密鍵を用いて作成し、この第２署名が付され暗号化された前記決済情報を、前記第２署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証可能な前記クライアント装置に送信して前記ＩＣカードに出力することを特徴とする、請求項１１記載の決済管理装置。

【請求項１３】 前記決済管理装置は、決済完了情報を生成し、この決済完了情報の正当性を示す第３署名を前記決済管理装置の秘密鍵を用いて生成し、前記決済情報を含むとともにこの第３署名が付された前記決済完了情報を、前記第３署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証可能な前記店舗装置に送信することを特徴とする、請求項１０記載の決済管理装置。

【請求項１４】 前記店舗装置は、前記第３署名が付された決済完了情報を

受信し、前記店舗装置の秘密鍵を用いて第4署名付き決済完了受領情報を生成し、この第4署名付き決済完了受領情報を前記決済管理装置に送信し、

前記決済管理装置は、前記店舗装置から受信した前記第4署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項第13記載の決済管理装置。

【請求項15】 コンピュータをして請求項8記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項16】 コンピュータをして請求項9記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項17】 コンピュータをして請求項10記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項18】 コンピュータをして請求項11記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項19】 コンピュータをして請求項12記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項20】 コンピュータをして請求項13記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項21】 コンピュータをして請求項14記載の決済管理装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項22】 請求項15記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項23】 請求項16記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項24】 請求項17記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項25】 請求項18記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項26】 請求項19記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 2 7】 請求項 2 0 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 2 8】 請求項 2 1 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 2 9】 決済管理装置を介して価値情報が記憶された I C カードとの間で行われる決済に基づいて、商品またはサービスを提供する店舗装置であって、

決済要求情報を生成する決済要求情報生成部と、

前記決済要求情報の正当性を示す第 1 署名を前記店舗装置の秘密鍵を用いて作成する第 1 署名生成部と、

前記第 1 署名が付された前記決済要求情報を、前記第 1 署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証可能な前記決済管理装置に送信する決済要求情報送信部とを備えたことを特徴とする、店舗装置。

【請求項 3 0】 前記決済管理装置は、前記 I C カードで決済を行うための決済情報を、前記店舗装置からの決済要求情報に基づいて生成し、前記決済情報を前記決済管理装置と前記 I C カードとの間で共用される共通鍵を用いて暗号化し、この暗号化された決済情報を前記クライアント装置に送信し、

前記クライアント装置は、前記決済管理装置から受信した前記決済情報を前記 I C カードに出力することを特徴とする、請求項 2 9 記載の店舗装置。

【請求項 3 1】 前記第 1 署名が付された前記決済要求情報は、前記店舗装置から前記クライアント装置を介して前記決済管理装置に送信されることを特徴とする、請求項 2 9 記載の店舗装置。

【請求項 3 2】 前記決済管理装置は、決済完了情報を生成し、この決済完了情報の正当性を示す第 3 署名を前記決済管理装置の秘密鍵を用いて生成し、前記決済情報を含むとともにこの第 3 署名が付された前記決済完了情報を前記店舗装置に送信し、

前記店舗装置は、前記決済管理装置から受信した前記第 3 署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項 2 9 記載の店舗装置。

【請求項 3 3】 前記店舗装置は、前記第 3 署名が付された決済完了情報を受信し、前記店舗装置の秘密鍵を用いて第 4 署名付き決済完了受領情報を生成し、この第 4 署名付き決済完了受領情報を前記決済管理装置および前記クライアント装置に送信し、

前記決済管理装置および前記クライアントは、前記店舗装置から受信した前記第 4 署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項第 3 2 記載の店舗装置。

【請求項 3 4】 前記店舗装置は、複数の下層店舗装置を含むモールとして構成されていることを特徴とする、請求項 2 9 記載の店舗装置。

【請求項 3 5】 コンピュータをして請求項 2 9 記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 3 6】 コンピュータをして請求項 3 0 記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 3 7】 コンピュータをして請求項 3 1 記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 3 8】 コンピュータをして請求項 3 2 記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 3 9】 コンピュータをして請求項 3 3 記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 4 0】 コンピュータをして請求項 3 4 記載の店舗装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 4 1】 請求項 3 5 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 4 2】 請求項 3 6 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 4 3】 請求項 3 7 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 4 4】 請求項 3 8 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 4 5】 請求項 3 9 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 4 6】 請求項 4 0 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 4 7】 商品またはサービスを提供する店舗装置と価値情報が記憶された IC カードとの間の決済を決済管理装置を介して行うに際して使用される前記 IC カードに対する情報入出力機能を備えたクライアント装置において、

前記決済管理装置が、前記店舗装置からの決済要求情報に基づいて生成し、前記決済管理装置と前記 IC カードとの間で共用される共通鍵を用いて暗号化した決済情報を受信する決済情報受信部と、

前記決済管理装置から受信した前記決済情報を前記 IC カードに出力する決済情報出力部とを備えていることを特徴とする、クライアント装置。

【請求項 4 8】 前記店舗装置は、前記決済要求情報の正当性を示す第 1 署名を前記店舗装置の秘密鍵を用いて作成し、前記第 1 署名が付された前記決済要求情報を前記クライアント装置を介して前記決済管理装置に送信し、

前記決済管理装置は、前記店舗装置から受信した前記第 1 署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項 4 7 記載のクライアント装置。

【請求項 4 9】 前記決済管理装置は、前記第 1 署名付き決済情報の正当性を示す第 2 署名を前記決済管理装置の秘密鍵を用いて作成し、この第 2 署名が付され暗号化された前記決済情報を前記クライアント装置に送信し、

前記クライアント装置は、前記決済管理装置から受信した前記第 2 署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記決済情報を前記 IC カードに出力することを特徴とする、請求項 4 8 記載のクライアント装置。

【請求項 5 0】 前記決済管理装置は、決済完了情報を生成し、この決済完了情報の正当性を示す第 3 署名を前記決済管理装置の秘密鍵を用いて生成し、前記決済情報を含むとともにこの第 3 署名が付された前記決済完了情報を前記店舗装置に送信し、

前記店舗装置は、前記決済管理装置から受信した前記第 3 署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証し、さらに前記店舗装置の秘密鍵を用いて第 4 署名付き決済完了受領情報を生成し、この第 4 署名付き決済完了受領情報を前記クライアント装置に送信し、

前記クライアントは、前記店舗装置から受信した前記第 4 署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項第 4 7 記載のクライアント装置。

【請求項 5 1】 コンピュータをして請求項 4 7 記載のクライアント装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 5 2】 コンピュータをして請求項 4 8 記載のクライアント装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 5 3】 コンピュータをして請求項 4 9 記載のクライアント装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 5 4】 コンピュータをして請求項 5 0 記載のクライアント装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 5 5】 請求項 5 1 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 5 6】 請求項 5 2 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 5 7】 請求項 5 3 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 5 8】 請求項 5 4 記載のコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 5 9】 商品またはサービスを提供する店舗装置との間の決済を決済管理装置を介して行うに際して使用される価値情報が記憶された IC カードにおいて

前記決済管理装置が、前記店舗装置からの決済要求情報に基づいて生成し、前記決済管理装置と前記 IC カードとの間で共用される共通鍵を用いて暗号化した決済情報を、前記 IC カードに対する情報入出力機能を備えた前記クライアント

装置を介して入力可能であることを特徴とする、ＩＣカード。

【請求項 6 0】 前記店舗装置は、前記決済要求情報の正当性を示す第 1 署名を前記店舗装置の秘密鍵を用いて作成し、前記第 1 署名が付された前記決済要求情報を前記決済管理装置に送信し、

前記決済管理装置は、前記店舗装置から受信した前記第 1 署名の正当性を前記店舗装置の秘密鍵に対応する公開鍵を用いて検証するとともに、前記第 1 署名付き決済情報の正当性を示す第 2 署名を前記決済管理装置の秘密鍵を用いて作成し、この第 2 署名が付され暗号化された前記決済情報を前記クライアント装置に送信し、

前記クライアント装置は、前記決済管理装置から受信した前記第 2 署名の正当性を前記決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記決済情報を前記ＩＣカードに出力することを特徴とする、請求項 5 9 記載のＩＣカード。

【請求項 6 1】 価値情報が記憶されたＩＣカード手段と、

前記ＩＣカードに対する情報入出力機能を備えたクライアント手段と、

商品またはサービスを提供する店舗手段であって、クライアント手段からの購入要求に応じて前記ＩＣカードによる決済情報を生成する店舗手段と、

前記ＩＣカードと前記店舗手段間の決済を管理する決済管理手段であって、前記ＩＣカードで決済を行うための決済情報を、前記店舗手段からの決済要求情報に基づいて生成し、前記決済情報を前記決済管理手段と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、この暗号化された決済情報を前記クライアント手段に送信する決済管理手段と、

前記クライアント手段と前記店舗手段と前記決済管理手段とを双方向通信可能に接続する通信系とから成ることを特徴とする、電子決済システム。

【請求項 6 2】 前記店舗手段は、前記決済要求情報の正当性を示す第 1 署名を前記店舗手段の秘密鍵を用いて作成し、前記第 1 署名が付された前記決済要求情報を前記決済管理手段に送信し、

前記決済管理手段は、前記店舗手段から受信した前記第 1 署名の正当性を前記店舗手段の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項

6 1 記載の電子決済システム。

【請求項 6 3】 前記第 1 署名が付された前記決済要求情報は、前記クライアント手段を介して前記決済管理手段に送信されることを特徴とする、請求項 6 2 記載の電子決済システム。

【請求項 6 4】 前記決済管理手段は、前記第 1 署名付き決済情報の正当性を示す第 2 署名を前記決済管理手段の秘密鍵を用いて作成し、この第 2 署名が付され暗号化された前記決済情報を前記クライアント手段に送信し、

前記クライアント手段は、前記決済管理手段から受信した前記第 2 署名の正当性を前記決済管理手段の秘密鍵に対応する公開鍵を用いて検証した後に、前記決済情報を前記 IC カードに出力することを特徴とする、請求項 6 2 記載の電子決済システム。

【請求項 6 5】 前記決済管理手段は、決済完了情報を生成し、この決済完了情報の正当性を示す第 3 署名を前記決済管理手段の秘密鍵を用いて生成し、前記決済情報を含むとともにこの第 3 署名が付された前記決済完了情報を前記店舗手段に送信し、

前記店舗手段は、前記決済管理手段から受信した前記第 3 署名の正当性を前記決済管理手段の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項 6 1 記載の電子決済システム。

【請求項 6 6】 前記店舗手段は、前記第 3 署名が付された決済完了情報を受信し、前記店舗手段の秘密鍵を用いて第 4 署名付き決済完了受領情報を生成し、この第 4 署名付き決済完了受領情報を前記決済管理手段および前記クライアント手段に送信し、

前記決済管理手段および前記クライアントは、前記店舗手段から受信した前記第 4 署名の正当性を前記店舗手段の秘密鍵に対応する公開鍵を用いて検証することを特徴とする、請求項第 6 1 記載の電子決済システム。

【請求項 6 7】 前記店舗手段は、複数の下層店舗手段を含むモールとして構成されていることを特徴とする、請求項 6 1 記載の電子決済システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】 本発明は、共通鍵を保持したＩＣカードを用いて、ネットワークなどを用いた決済処理を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカード、コンピュータプログラムおよび記憶媒体に関する。

【 0 0 0 2 】

【従来の技術】 インターネットなどのオープンネットワークを介した電子商取引を安全に行うために、従来、PKI (Public Key Infrastructure : 公開鍵インフラ) プロトコルが採用されている。

【 0 0 0 3 】

PKI プロトコルでは、送信元で秘密鍵を用いて署名情報を作成し、送信元から送信先に、当該署名情報を伝送情報と共に送信する。そして、送信先において、当該秘密鍵に対応する公開鍵を用いて当該署名情報の検証を行うことで、受信した伝送情報が正当な送信元で作成されたものであるか否かを判断する。

【 0 0 0 4 】

ところで、近年、IC (Integrated Circuit) カードを用いて、ネットワークを介した電子商取引を行う試みがある。ここで、通常、IC カードは、共通鍵を保持しており、共通鍵暗号方式を用いて秘匿性のある情報の入出力を行う。このようなIC カードは、共通鍵が署名情報を作成するための鍵とはなり得ないため、IC カードを紛失した場合でも、被害を小さくできるという利点がある。

【 0 0 0 5 】

【発明の解決しようとする課題】 しかしながら、ネットワークを介した電子商取引を安全に行うためには、秘密鍵を用いて署名情報を作成する必要があるが、従来の手法では、IC カードが秘密鍵を保持（記憶）していないため、署名情報の作成ができないという問題がある。この場合に、IC カードに秘密鍵を保持する方法も考えられるが、前述したように、秘密鍵は署名情報を作成できるため印鑑照明と同様の効力があり、IC カードを紛失して悪用されたときの被害が大きすぎるという問題がある。

【 0 0 0 6 】

また、上述したようなＩＣカードが採用する共通鍵暗号方式のみを用いて、ネットワークを介した電子商取引を行うと、取引を行う多数の相手先のサーバ装置などが共通鍵を持つことになり、共通鍵が盗まれたり、悪用される可能性が高くなるという問題もある。

【0007】

従来の電子決済においては、SSL (Secure Socket Layer) やSET (Secure Electronic Transaction) が多く採用されている。しかし、SSLでは、クライアント装置と店舗装置間の通信路に対する安全性は保証されるが、店舗側の不正を検出できないという問題がある。

【0008】

また、SETでは、SSLの利点とクライアント装置、店舗装置、決済管理装置で改ざんができないという利点とを併せ持つが、各装置がPKIの証明書を持たなければならないため、煩雑であり費用がかかり、さらに署名および署名検証を何度も行わなければならない冗長であるという問題がある。

【0009】

さらに、従来の電子商取引システムにおいては、ユーザがクライアント装置上で確認した価値情報が、実際にＩＣカードに書き込まれる価値情報と同じであるかどうかを確認する手段を持っていなかった。

【0010】

本発明は上述した従来技術の問題点に鑑みてなされ、共通鍵を保持したＩＣカードを用いて、ネットワークを介した電子商取引を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカード、コンピュータプログラムおよび記憶媒体を提供することを目的とする。

【0011】

【課題を解決するための手段】

上記課題を解決するために、本発明によれば、新規かつ改良された電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカード、コンピュータプログラムおよび記憶媒体が提供される。

【 0 0 1 2 】

本発明の第1の観点によれば、価値情報が記憶されたICカードと、ICカードに対する情報入出力機能を備えたクライアント装置と、商品またはサービスを提供する店舗装置と、ICカードと店舗装置間の決済を管理する決済管理装置と、クライアント装置と店舗装置と決済管理装置とを双方向通信可能に接続する通信系とから成る電子決済システムであって、決済管理装置は、ICカードで決済を行うための決済情報を、店舗装置からの決済要求情報に基づいて生成し、決済情報を決済管理装置とICカードとの間で共用される共通鍵を用いて暗号化し、この暗号化された決済情報をクライアント装置に送信し、クライアント装置は、決済管理装置から受信した決済情報をICカードに出力することを特徴とする、電子決済システムが提供される。

【 0 0 1 3 】

上記電子決済システムにおいて、店舗装置は、決済要求情報の正当性を示す第1署名を店舗装置の秘密鍵を用いて作成し、第1署名が付された決済要求情報を決済管理装置に送信し、決済管理装置は、店舗装置から受信した第1署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【 0 0 1 4 】

第1署名が付された決済要求情報は、クライアント装置を介して決済管理装置に送信されることが好ましい。

【 0 0 1 5 】

決済管理装置は、第1署名付き決済情報の正当性を示す第2署名を決済管理装置の秘密鍵を用いて作成し、この第2署名が付され暗号化された決済情報をクライアント装置に送信し、クライアント装置は、決済管理装置から受信した第2署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に、決済情報をICカードに出力することが好ましい。

【 0 0 1 6 】

決済管理装置は、決済完了情報を生成し、この決済完了情報の正当性を示す第3署名を決済管理装置の秘密鍵を用いて生成し、決済情報を含むとともにこの第3署名が付された決済完了情報を店舗装置に送信し、

【 0 0 1 7 】

店舗装置は、決済管理装置から受信した第 3 署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【 0 0 1 8 】

店舗装置は、第 3 署名が付された決済完了情報を受信し、店舗装置の秘密鍵を用いて第 4 署名付き決済完了受領情報を生成し、この第 4 署名付き決済完了受領情報を決済管理装置およびクライアント装置に送信し、決済管理装置およびクライアント装置は、店舗装置から受信した第 4 署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【 0 0 1 9 】

店舗装置は、単一の店舗装置として構成しても良いし、複数の下層店舗装置を含むモールとして構成しても良い。

【 0 0 2 0 】

さらに本発明の別の観点によれば、ＩＣカードに記憶されている価値情報をクライアント装置を介して更新することが可能な決済管理装置において、決済管理装置は、ＩＣカードの価値更新情報を決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化し、この暗号化された価値更新情報をクライアント装置に送信し、クライアント装置は、受信した価値更新情報をＩＣカードに入力することを特徴とする、決済管理装置が提供される。

【 0 0 2 1 】

決済管理装置は、価値更新情報の正当性を示す第 5 署名を決済管理装置の秘密鍵を用いて生成し、第 5 署名が付された価値更新情報をクライアント装置に送信し、クライアント装置は、決済管理装置から受信した第 5 署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に、価値更新情報をＩＣカードに入力することが好ましい。

【 0 0 2 2 】

価値情報が記憶されたＩＣカードと商品またはサービスを提供する店舗装置との間の決済を管理する決済管理装置において、ＩＣカードで決済を行うための決済情報を、店舗装置からの決済要求情報に基づいて生成する決済情報生成部と、

決済情報を決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化する決済情報暗号化部と、この暗号化された決済情報をＩＣカードに対する情報入出力機能を備えたクライアント装置を介してＩＣカードに出力する決済情報出力部とを備えたことが好ましい。

【 0 0 2 3 】

店舗装置は、決済要求情報の正当性を示す第１署名を店舗装置の秘密鍵を用いて作成し、第１署名が付された決済要求情報を決済管理装置に送信し、決済管理装置は、店舗装置から受信した第１署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【 0 0 2 4 】

決済管理装置は、第１署名付き決済情報の正当性を示す第２署名を決済管理装置の秘密鍵を用いて作成し、この第２署名が付され暗号化された決済情報を、第２署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証可能なクライアント装置に送信してＩＣカードに出力することが好ましい。

【 0 0 2 5 】

決済管理装置は、決済完了情報を生成し、この決済完了情報の正当性を示す第３署名を決済管理装置の秘密鍵を用いて生成し、決済情報を含むとともにこの第３署名が付された決済完了情報を、第３署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証可能な店舗装置に送信することが好ましい。

【 0 0 2 6 】

店舗装置は、第３署名が付された決済完了情報を受信し、店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し、この第４署名付き決済完了受領情報を決済管理装置に送信し、決済管理装置は、店舗装置から受信した第４署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【 0 0 2 7 】

さらに、本発明の別の観点によれば、コンピュータをして上記決済管理装置として機能せしめることを特徴とするコンピュータプログラムが提供される。

【 0 0 2 8 】

また、本発明の別の観点によれば、コンピュータをして上記決済管理装置として機能せしめることを特徴とする上記コンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体が提供される。

【 0 0 2 9 】

さらにまた、本発明の別の観点によれば、決済管理装置を介して価値情報が記憶されたＩＣカードとの間で行われる決済に基づいて、商品またはサービスを提供する店舗装置であって、決済要求情報を生成する決済要求情報生成部と、決済要求情報の正当性を示す第１署名を店舗装置の秘密鍵を用いて作成する第１署名生成部と、第１署名が付された決済要求情報を、第１署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証可能な決済管理装置に送信する決済要求情報送信部とを備えたことを特徴とする、店舗装置が提供される。

【 0 0 3 0 】

決済管理装置は、ＩＣカードで決済を行うための決済情報を、店舗装置からの決済要求情報に基づいて生成し、決済情報を決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化し、この暗号化された決済情報をクライアント装置に送信し、クライアント装置は、決済管理装置から受信した決済情報をＩＣカードに出力することが好ましい。

【 0 0 3 1 】

第１署名が付された決済要求情報は、店舗装置からクライアント装置を介して決済管理装置に送信されることが好ましい。

【 0 0 3 2 】

決済管理装置は、決済完了情報を生成し、この決済完了情報の正当性を示す第３署名を決済管理装置の秘密鍵を用いて生成し、決済情報を含むとともにこの第３署名が付された決済完了情報を店舗装置に送信し、店舗装置は、決済管理装置から受信した第３署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【 0 0 3 3 】

店舗装置は、第３署名が付された決済完了情報を受信し、店舗装置の秘密鍵を用いて第４署名付き決済完了受領情報を生成し、この第４署名付き決済完了受領

情報を決済管理装置およびクライアント装置に送信し、決済管理装置およびクライアントは、店舗装置から受信した第4署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【 0 0 3 4 】

店舗装置は、単一の店舗装置として構成しても良いし、複数の下層店舗装置を含むモールとして構成しても良い。

【 0 0 3 5 】

さらに、本発明の別の観点によれば、コンピュータをして上記店舗装置として機能せしめることを特徴とするコンピュータプログラムが提供される。

【 0 0 3 6 】

また、本発明の別の観点によれば、コンピュータをして上記店舗装置として機能せしめることを特徴とする上記コンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体が提供される。

【 0 0 3 7 】

さらにまた、本発明の別の観点によれば、商品またはサービスを提供する店舗装置と価値情報が記憶されたICカードとの間の決済を決済管理装置を介して行うに際して使用されるICカードに対する情報入出力機能を備えたクライアント装置において、決済管理装置が、店舗装置からの決済要求情報に基づいて生成し、決済管理装置とICカードとの間で共用される共通鍵を用いて暗号化した決済情報を受信する決済情報受信部と、決済管理装置から受信した決済情報をICカードに出力する決済情報出力部とを備えていることを特徴とする、クライアント装置が提供される。

【 0 0 3 8 】

店舗装置は、決済要求情報の正当性を示す第1署名を店舗装置の秘密鍵を用いて作成し、第1署名が付された決済要求情報をクライアント装置を介して決済管理装置に送信し、決済管理装置は、店舗装置から受信した第1署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【 0 0 3 9 】

決済管理装置は、第1署名付き決済情報の正当性を示す第2署名を決済管理装

置の秘密鍵を用いて作成し、この第2署名が付され暗号化された決済情報をクライアント装置に送信し、クライアント装置は、決済管理装置から受信した第2署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に、決済情報をICカードに出力することが好ましい。

【0040】

決済管理装置は、決済完了情報を生成し、この決済完了情報の正当性を示す第3署名を決済管理装置の秘密鍵を用いて生成し、決済情報を含むとともにこの第3署名が付された決済完了情報を店舗装置に送信し、店舗装置は、決済管理装置から受信した第3署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証し、さらに店舗装置の秘密鍵を用いて第4署名付き決済完了受領情報を生成し、この第4署名付き決済完了受領情報をクライアント装置に送信し、クライアントは、店舗装置から受信した第4署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【0041】

さらに、本発明の別の観点によれば、コンピュータをして上記クライアント装置として機能せしめることを特徴とするコンピュータプログラムが提供される。

【0042】

また、本発明の別の観点によれば、コンピュータをして上記クライアント装置として機能せしめることを特徴とする上記コンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体が提供される。

【0043】

さらに本発明の別の観点によれば、商品またはサービスを提供する店舗装置との間の決済を決済管理装置を介して行うに際して使用される価値情報が記憶されたICカードにおいて、決済管理装置が、店舗装置からの決済要求情報に基づいて生成し、決済管理装置とICカードとの間で共用される共通鍵を用いて暗号化した決済情報を、ICカードに対する情報入出力機能を備えたクライアント装置を介して入力可能であることを特徴とする、ICカードが提供される。

【0044】

店舗装置は、決済要求情報の正当性を示す第1署名を店舗装置の秘密鍵を用い

て作成し、第 1 署名が付された決済要求情報を決済管理装置に送信し、決済管理装置は、店舗装置から受信した第 1 署名の正当性を店舗装置の秘密鍵に対応する公開鍵を用いて検証するとともに、第 1 署名付き決済情報の正当性を示す第 2 署名を決済管理装置の秘密鍵を用いて作成し、この第 2 署名が付され暗号化された決済情報をクライアント装置に送信し、クライアント装置は、決済管理装置から受信した第 2 署名の正当性を決済管理装置の秘密鍵に対応する公開鍵を用いて検証した後に、決済情報を IC カードに出力することが好ましい。

【 0 0 4 5 】

さらに、本発明の別の観点によれば、価値情報が記憶された IC カード手段と、IC カードに対する情報入出力機能を備えたクライアント手段と、商品またはサービスを提供する店舗手段であって、クライアント手段からの購入要求に応じて IC カードによる決済情報を生成する店舗手段と、IC カードと店舗手段間の決済を管理する決済管理手段であって、IC カードで決済を行うための決済情報を、店舗手段からの決済要求情報に基づいて生成し、決済情報を決済管理手段と IC カードとの間で共用される共通鍵を用いて暗号化し、この暗号化された決済情報をクライアント手段に送信する決済管理手段と、クライアント手段と店舗手段と決済管理手段とを双方向通信可能に接続する通信系とから成ることを特徴とする、電子決済システムが提供される。

【 0 0 4 6 】

店舗手段は、決済要求情報の正当性を示す第 1 署名を店舗手段の秘密鍵を用いて作成し、第 1 署名が付された決済要求情報を決済管理手段に送信し、決済管理手段は、店舗手段から受信した第 1 署名の正当性を店舗手段の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【 0 0 4 7 】

第 1 署名が付された決済要求情報は、クライアント手段を介して決済管理手段に送信されることが好ましい。

【 0 0 4 8 】

決済管理手段は、第 1 署名付き決済情報の正当性を示す第 2 署名を決済管理手段の秘密鍵を用いて作成し、この第 2 署名が付され暗号化された決済情報をクラ

クライアント手段に送信し、クライアント手段は、決済管理手段から受信した第2署名の正当性を決済管理手段の秘密鍵に対応する公開鍵を用いて検証した後に、決済情報をICカードに出力することが好ましい。

【0049】

決済管理手段は、決済完了情報を生成し、この決済完了情報の正当性を示す第3署名を決済管理手段の秘密鍵を用いて生成し、決済情報を含むとともにこの第3署名が付された決済完了情報を店舗手段に送信し、

【0050】

店舗手段は、決済管理手段から受信した第3署名の正当性を決済管理手段の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【0051】

店舗手段は、第3署名が付された決済完了情報を受信し、店舗手段の秘密鍵を用いて第4署名付き決済完了受領情報を生成し、この第4署名付き決済完了受領情報を決済管理手段およびクライアント手段に送信し、決済管理手段およびクライアントは、店舗手段から受信した第4署名の正当性を店舗手段の秘密鍵に対応する公開鍵を用いて検証することが好ましい。

【0052】

店舗手段は、単一の店舗手段として構成しても良いし、複数の下層店舗手段を含むモールとして構成しても良い。

【0053】

ここで、発明の理解を容易にするために、本発明に共通の用語について簡単に整理して説明する。

【0054】

「電子決済システム」は、インターネットなどのオンライン通信系を介して商品やサービスの販売を行った場合に、代金決済を電子的にオンライン通信系を介して行うシステムである。オンライン通信系を介して決済を行う方法としては、クレジットカードやキャッシュカードやデビットカードによる支払い、プリペイドカードなどの電子マネーによる支払いが可能である。

【0055】

「ＩＣカード」は、例えば、プラスチックなどのカードにＩＣチップが埋め込まれているものをいう。メモリチップのみを持っているタイプをメモリカードと呼び、ＣＰＵも搭載しているタイプはＣＰＵ内蔵カードと呼ばれる。さらに、ＩＣカードはＣＰＵの有無による種類のほかに、リーダライタに対する「接触」「非接触」でも区分できる。接触型は表面に金属の端子が載っていて、その端子を通してリーダライタと電力の供給やデータのやりとりを行う。それに対して、内部にアンテナを持ち、そのアンテナを通して電力供給やデータの読み取り／書き込みをするのが非接触型である。

【 0 0 5 6 】

「価値情報」は、ＩＣカードに記憶されて、商品やサービスの提供に対する対価として交換可能な価値に関する情報である。価値情報には、通貨に相当する貨幣的価値を有するものや、ポイントなどように商品やサービスと交換可能な擬似貨幣的価値を有するものが含まれる。

【 0 0 5 7 】

「クライアント装置」は、少なくともＩＣカードに対する情報入出力機能とインターネットなどのオンライン通信系を介して他の端末装置やサーバと双方向通信可能な機能を有する端末装置である。「クライアント装置」は、一般的には、演算装置、記憶装置、表示装置、入出力装置、通信装置、ＩＣカードリーダライタなどを備えたコンピュータ装置であり、同様の機能を有する携帯端末装置や携帯電話装置などを含む。クライアント装置の設置場所は、ユーザの家庭あるいは職場でも構わないし、あるいは本決済システム専用のクライアント端末が設置された店舗でも構わない。

【 0 0 5 8 】

「店舗装置」は、例えばインターネットなどのオンライン通信系を介して商品やサービスを販売等提供するネットワークサーバである。店舗装置は単一のネットワークサーバから構成しても、複数のネットワークサーバから構成されるモジュールとして構成しても構わない。

【 0 0 5 9 】

「決済管理装置」は、例えばＩＣカードと店舗装置間の決済を管理する管理サ

ーバであり、セキュリティサーバ、アプリケーションサーバ、データベースサーバなどから構成される。

【 0 0 6 0 】

「通信系」は、所定の通信プロトコルを介して双方向通信可能に構成された、例えば公衆回線網を利用したインターネットや、LAN (Local Area Network) やWAN (Wide Area Network) などのオンライン通信系であり、接続形態は有線無線を問わない。

【 0 0 6 1 】

「決済要求情報」は、店舗装置が作成するもので、ユーザがクライアント装置を介して店舗装置に送信した購買要求に対する決済を決済管理装置に要求するための各種情報が含まれる。この決済要求情報の正当性は、店舗装置の秘密鍵を用いて作成された第1署名を付し、決済管理装置がその第1署名を店舗装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【 0 0 6 2 】

「決済情報」は、決済管理装置が店舗装置から決済管理装置に送信された決済要求情報に基づいて作成するもので、決済管理装置からクライアント装置を介してICカードに記憶された価値情報を増減することにより決済を行うための各種情報が含まれる。この決済情報のセキュリティは、決済管理装置とICカードとの間で共用される共通鍵により確保される。さらに、決済情報の正当性は、決済管理装置の秘密鍵を用いて作成された第2署名を付し、クライアント装置がその第2署名を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【 0 0 6 3 】

「決済完了情報」は、決済管理装置がICカードに記憶された価値情報を増減することにより決済が行われたことを確認した後に生成され、店舗装置に送信されるもので、決済完了に関する各種情報が含まれる。この決済完了情報の正当性は、決済管理装置の秘密鍵を用いて生成された第3署名を付し、店舗装置がその第3署名を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【 0 0 6 4 】

「決済完了受領情報」は、店舗装置がユーザが所有するＩＣカードに基づいて決済が完了したことを確認した後に生成されて、決済管理装置およびクライアント装置に送信されるもので、これにより決済の完了が確認され、店舗からユーザに対して商品またはサービスの受け渡しが可能となる。この決済完了情報の正当性は、店舗装置の秘密鍵を用いて生成された第４署名を付し、決済管理装置およびクライアント装置が店舗装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【 0 0 6 5 】

「価値更新情報」は、ＩＣカードに記憶されている価値情報を増減するための情報であり、決済管理装置からクライアント装置を介してＩＣカードに入力される。この価値更新情報のセキュリティは、決済管理装置とＩＣカードとの間で共用される共通鍵により確保される。さらに、価値更新情報の正当性は、決済管理装置の秘密鍵を用いて作成された第５署名を付し、クライアント装置がその第５署名を決済管理装置の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【 0 0 6 6 】

「共通鍵」は、いわゆる共通鍵暗号化方式で、暗号化と復号化の双方に用いられる鍵であり、送り手と受け手が鍵を共用するものである。本発明においては、決済管理装置とＩＣカードとの間において共通鍵が設定される。

【 0 0 6 7 】

「秘密鍵」は、いわゆる公開鍵暗号化方式で暗号化に用いられる鍵であり、秘密鍵により暗号化された情報は、認証局などに保管されている対応する公開鍵により復号化が可能となる。

【 0 0 6 8 】

「公開鍵」は、いわゆる公開鍵暗号化方式で復号化に用いられる鍵であり、通常は、認証局などに保管されており、受信者は、秘密鍵により暗号化された情報を復号化する際に、認証局から公開鍵を入手して復号化を行うものである。

【 0 0 6 9 】

「電子署名」は、送信される情報の正当性を保証するものであるが、送信側と受信側との種類に応じて、本発明においては第1署名～第5署名が使用される。

【0070】

「第1署名」は、店舗装置の秘密鍵により作成され、決済要求情報に付されて、決済管理装置において、対応する公開鍵を用いて検証される署名である。

【0071】

「第2署名」は、決済管理装置の秘密鍵により作成され、決済情報に付されて、クライアント装置において、対応する公開鍵を用いて検証される署名である。

【0072】

「第3署名」は、決済管理装置の秘密鍵により作成され、決済完了情報に付されて、店舗装置において、対応する公開鍵を用いて検証される署名である。

【0073】

「第4署名」は、店舗装置の秘密鍵により作成され、決済完了受領情報に付されて、決済管理装置において、対応する公開鍵を用いて検証される署名である。

【0074】

「第5署名」は、決済管理装置の秘密鍵により作成され、価値更新求情報に付されて、クライアント装置において、対応する公開鍵を用いて検証される署名である。

【0075】

【発明の実施の形態】 以下、添付図面を参照しながら、本発明の好適な実施形態にかかる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカード、コンピュータプログラムおよび記憶媒体について説明する。

【0076】

図1は、本実施形態にかかる電子決済システムを適用可能な電子決済システム1の全体構成図である。

【0077】

図1に示すように、電子決済システム1は、クライアント装置およびＩＣカードを含むユーザ2、決済管理装置3および店舗装置4の間で、所定の通信プロトコルを介して双方向通信可能な通信系であるインターネットなどのネットワーク

5を介した通信を行うことが可能である。

【0078】

〔ユーザ2〕

ユーザ2には、ICカード20と、ICカード20にアクセスして情報の入出力を行うリーダライタ装置21およびパーソナルコンピュータ22などから構成されるクライアント装置が設けられている。

【0079】

ICカード20は、例えば、プラスチックなどのカードにICチップが埋め込まれているものである。ICカード20は、図2（A）に示すように耐タンパ性のICモジュール50を有し、図2（B）に示すように当該ICモジュール50内に処理回路51およびメモリ52を内蔵している。

【0080】

ICカード20の処理回路51は、決済管理装置3のセキュリティサーバ31との間で共用される共通鍵KCを用いた復号処理、所定の情報および要求に応じた処理、並びに相互認証処理などの種々の処理を行うことが可能である。

【0081】

メモリ52は、決済管理装置3のセキュリティサーバ31との間で共用する共通鍵KCを記憶している。

【0082】

ICカード20は、図3に示すように、ICカードリーダライタ21を介してパーソナルコンピュータ22と通信を行い、パーソナルコンピュータ22内で駆動するActiveXコンポーネントなどのインタフェースプログラム24やブラウザプログラム23を介して、インターネットなどのネットワーク5に接続する。さらに、ICカード20は、決済管理装置3のアプリケーションサーバ30を介して、セキュリティサーバ31に接続し、セキュリティサーバ31との間で情報を送受信する。このように確立されるICカード20とセキュリティサーバ31との間の情報通信は、共通鍵KCを用いた共通鍵暗号化方式（PKIプロトコル）によって暗号化および復号化されることにより、セキュリティが確保されている。

【 0 0 8 3 】

なお、ICカードには、価値情報が記憶されている。この価値情報は、商品やサービスの提供に対する対価として交換可能な価値に関する情報である。価値情報には、通貨に相当する貨幣的価値を有するものや、ポイントなどように商品やサービスと交換可能な擬似貨幣的価値を有するものが含まれる。

【 0 0 8 4 】

ICカードのリーダライタ21は、ICカード20のICモジュール50との間で非接触方式あるいは接触方式でデータ入出力を行うと共に、パーソナルコンピュータ22との間との間で情報および要求の入出力を行うものである。

【 0 0 8 5 】

パーソナルコンピュータ22は、ユーザによるキーボードやマウスなどの操作に応じて、ブラウザプログラム23を実行すると共に、ブラウザプログラム23上で、後述するようにネットワーク5を介して決済管理装置3のアプリケーションサーバ30から受信したActiveXコンポーネントなどのインタフェースプログラム24を実行する。

【 0 0 8 6 】

パーソナルコンピュータ22は、ディスプレイ、キーボードおよびマウスなどを有している。なお、図示の例では、クライアント装置の例として、リーダライタ21が接続可能なパーソナルコンピュータ22を挙げているが、ICカードとの間で接触または非接触に情報交換を行うことが可能な機器であれば、パーソナルコンピュータ22に限定されず、携帯端末装置や携帯電話端末装置などを使用することも可能である。

【 0 0 8 7 】

ブラウザプログラム23は、図4に示すように、例えば、マイクロソフト社のインターネットエクスプローラなどのようにパーソナルコンピュータ22上で動作して、ネットワークサーバが提供するサービスをクライアント側の端末上で表示させることが可能なプログラムである。本実施の形態においては、ブラウザプログラム23は、店舗装置4のネットワークサーバ40のHTTPSレイヤ60との間で、PKIプロトコルにより、送信元において自らの秘密鍵を用いた署

名情報の付加，並びに送信先において当該秘密鍵に対応する公開鍵を用いた当該署名情報の検証を行う。

【 0 0 8 8 】

インタフェースプログラム 2 4 は，図 5 に示すように，パーソナルコンピュータ 2 2 上で動作し，決済管理装置 3 のアプリケーションサーバ 3 0 の A P S 上位レイヤ 3 0 a との間で，P K I プロトコルにより，送信元において自らの秘密鍵を用いた署名情報の付加，並びに送信先において当該秘密鍵に対応する公開鍵を用いた当該署名情報の検証を行うことが可能なプログラムである。

【 0 0 8 9 】

また，インタフェースプログラム 2 4 は，ブラウザプログラム 2 3 を実行中に，リーダライタ 2 1 を介して I C カード 2 0 などのローカル資源へのアクセスを容易に実現するための機能拡張プログラムとしても機能する。

【 0 0 9 0 】

〔決済管理装置 3〕

決済管理装置 3 には，図 1 および図 6 に示すように，バーチャル電子マネーシステムとして機能するアプリケーションサーバ 3 0，セキュリティ管理システムとして機能するセキュリティサーバ 3 1，精査・決済システムとして機能する情報管理サーバ 3 2，さらに本実施の形態とは直接的な関係はないが，リアル電子マネーシステムとして機能するアプリケーションサーバ 3 3 が設けられている。

【 0 0 9 1 】

決済管理装置 3 のアプリケーションサーバ 3 0 は，インターネットなどのネットワーク 5 を介して，ユーザ 2 のパーソナルコンピュータ 2 2 や店舗装置 4 のネットワークサーバ 4 0 と双方向通信が可能である。

【 0 0 9 2 】

また，決済管理装置 3 のアプリケーションサーバ 3 0 は，店舗装置 4 のネットワークサーバ 4 0 の秘密鍵 K S H O P , S に対応した公開鍵 K S H O P , P を保持し，後述するように，店舗装置 4 のネットワークサーバ 4 0 が生成した決済要求情報 B I L L に付された第 1 署名情報 S I G 1 を検証する。

【 0 0 9 3 】

さらに、決済管理装置 3 のアプリケーションサーバ 3 0 は、図 5 に示すように、A P S 上位レイヤ 3 0 a および A P S 下位レイヤ 3 0 b を有する。

【 0 0 9 4 】

決済管理装置 3 のセキュリティサーバ 3 1 は、ユーザ 2 の I C カード 2 0 との間で共用する共通鍵 K C を記憶している。

【 0 0 9 5 】

決済管理装置 3 のセキュリティサーバ 3 1 は、図 5 に示すように、I C カードのリーダライタ 2 1、インタフェースプログラム 2 4、ブラウザプログラム 2 3、パーソナルコンピュータ 2 2、ネットワーク 5 およびアプリケーションサーバ 3 0 を介して、I C カード 2 0 との間で送受信する情報を、共通鍵 K C を用いた共通鍵暗号方式によって暗号化および復号する。

【 0 0 9 6 】

情報管理サーバ 3 2 は、例えば、登録されたユーザの個人情報を記憶および管理する。

【 0 0 9 7 】

〔店舗装置 4〕

店舗装置 4 には、ネットワークサーバ 4 0 が設けられている。

【 0 0 9 8 】

店舗装置 4 のネットワークサーバ 4 0 は、図 4 に示すように、パーソナルコンピュータ 2 2 上で動作するブラウザプログラム 2 3 と H T T P S レイヤの間で、P K I プロトコルを介して双方向通信することが可能なように構成されている。

【 0 0 9 9 】

また、店舗装置 4 のネットワークサーバ 4 0 は、例えば、商品あるいはサービスの紹介情報を記憶すると共に、店舗装置 4 がユーザ 2 に請求する金額に対応する決済を要求する決済要求情報 B I L L と、当該決済要求情報に対して自らの秘密鍵 K S H O P , S を用いて作成した第 1 署名情報 S I G とを生成する。

【 0 1 0 0 】

店舗装置 4 は、図 6 に示すように単一の加盟店 4 2 として構成することが可能である。あるいは、店舗装置 4 は、図 6 に示すように、モール 4 1 の加盟店とし

て構成される加盟店 4 2 として構成することも可能である。

【 0 1 0 1 】

なお、図 6 に示す電子決済システムの構成例においては、ユーザがパーソナルコンピュータ 2 2 などを介してバーチャルにショッピングを行う際の決済に適用されるバーチャル電子マネーシステム 3 0 に加えて、ユーザが実際に店舗 7 に出かけてリアルにショッピングを行う際の決済に適用されるリアル電子マネーシステム 3 3 も含んでいる。

【 0 1 0 2 】

リアル電子マネーシステム 3 3 に対しては、公衆回線網 6 などの通信系を介して、ユーザが実際に訪問可能なリアル店舗 7 が接続されている。リアル店舗 7 は、独立店舗 7 1 として構成することも可能であり、あるいは本部 7 2 に従属する従属店舗 7 2 として構成することも可能である。ただし、リアル電子マネーシステム 3 3 については、本発明の要旨とは異なるので詳細説明は省略する。

【 0 1 0 3 】

次に図 7 を参照しながら、本実施の形態にかかる決済システムにおける情報の流れについて説明する。

【 0 1 0 4 】

すでに説明したように、本実施の形態にかかる決済システムにおいては、情報の受け手および送り手は、決済管理装置 3、店舗装置 4、パーソナルコンピュータ 2 2 およびリーダライタ 2 1 から成るクライアント装置 2 および IC カード 2 0 である。

【 0 1 0 5 】

上記情報の受け手および送り手間において流通する情報は、購買要求情報、決済要求情報、決済情報、決済完了情報、決済完了受領情報、価値更新情報などがある。

【 0 1 0 6 】

「購買要求情報」は、ユーザがクライアント装置であるパーソナルコンピュータ 2 2 のブラウザ 2 3 を介して店舗装置 4 のネットワークサーバ 4 0 にアクセスし、店舗装置 4 のサイトが展開する商品やサービスの中から、購入したい商品ま

たはサービスを選択し、店舗装置4に送信する情報である。

【0107】

「決済要求情報」は、店舗装置4が作成するもので、ユーザがクライアント装置であるパーソナルコンピュータ22を介して店舗装置に送信した購買要求情報に対する決済を決済管理装置3に要求するための各種情報が含まれる。この決済要求情報の正当性は、店舗装置4の秘密鍵を用いて作成された第1署名を付し、決済管理装置3がその第1署名を店舗装置4の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【0108】

「決済情報」は、決済管理装置3が店舗装置4から決済管理装置3に送信された決済要求情報に基づいて作成するもので、決済管理装置3からクライアント装置であるパーソナルコンピュータ22およびリーダライタ21を介してICカード20に記憶された価値情報を増減することにより決済を行うための各種情報が含まれる。この決済情報のセキュリティは、決済管理装置3とICカード20との間で共用される共通鍵により確保される。さらに、決済情報の正当性は、決済管理装置3の秘密鍵を用いて作成された第2署名を付し、クライアント装置であるパーソナルコンピュータ22がその第2署名を決済管理装置3の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【0109】

「決済完了情報」は、決済管理装置3がICカード20に記憶された価値情報を増減することにより決済が行われたことを確認した後に生成され、店舗装置4に送信されるもので、決済完了に関する各種情報が含まれる。この決済完了情報の正当性は、決済管理装置3の秘密鍵を用いて生成された第3署名を付し、店舗装置4がその第3署名を決済管理装置3の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【0110】

「決済完了受領情報」は、店舗装置4がユーザが所有するICカード20に基づいて決済が完了したことを確認した後に生成されて、決済管理装置3およびクライアント装置であるパーソナルコンピュータ22に送信されるもので、これに

より決済の完了が確認され、店舗装置4からユーザに対して商品またはサービスの受け渡しが可能となる。この決済完了情報の正当性は、店舗装置4の秘密鍵を用いて生成された第4署名を付し、決済管理装置3およびクライアント装置であるパーソナルコンピュータ22が店舗装置4の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【0111】

「価値更新情報」は、ICカード20に記憶されている価値情報を増減するための情報であり、決済管理装置3からクライアント装置であるパーソナルコンピュータ22およびリーダライタ21を介してICカード20に入力される。この価値更新情報のセキュリティは、決済管理装置3とICカード20との間で共用される共通鍵により確保される。さらに、価値更新情報の正当性は、決済管理装置3の秘密鍵を用いて作成された第5署名を付し、クライアント装置であるパーソナルコンピュータ22がその第5署名を決済管理装置3の秘密鍵に対応する公開鍵を用いて検証することにより確保される。

【0112】

なお、本実施の形態にかかる決済システムにおいて、送信される情報の正当性を保証するために用いられる電子署名は、送信側と受信側との種類に応じて、第1署名～第5署名が使用される。

【0113】

「第1署名」は、店舗装置4の秘密鍵により作成され、決済要求情報に付されて、決済管理装置3において、対応する公開鍵を用いて検証される署名である。

【0114】

「第2署名」は、決済管理装置3の秘密鍵により作成され、決済情報に付されて、クライアント装置であるパーソナルコンピュータ22において、対応する公開鍵を用いて検証される署名である。

【0115】

「第3署名」は、決済管理装置3の秘密鍵により作成され、決済完了情報に付されて、店舗装置4において、対応する公開鍵を用いて検証される署名である。

【0116】

「第4署名」は、店舗装置4の秘密鍵により作成され、決済完了受領情報に付されて、決済管理装置3において、対応する公開鍵を用いて検証される署名である。

【0117】

「第5署名」は、決済管理装置3の秘密鍵により作成され、価値更新求情報に付されて、クライアント装置であるパーソナルコンピュータ22において、対応する公開鍵を用いて検証される署名である。

【0118】

次に、図8を参照しながら、本実施の形態にかかる決済システムにおける電子マネー出金動作について説明する。

【0119】

ユーザ2は、パーソナルコンピュータ22を介して加盟店42の根とワークサーバ40にアクセスし、サイトにおいて提供される商品またはサービスの中から、ユーザ2が購入を希望する商品またはサービスの選択を行う(①)。

【0120】

加盟店42は、ユーザ2が選択した商品またはサービスの合計金額に関する情報をユーザに送信する(②)。

【0121】

ユーザ2は、加盟店42が所属するモール41に対して、本実施の形態にかかる決済システムを利用し電子マネーによる決済を依頼する(③)。

【0122】

ユーザ2からの電子マネー決済依頼を受けて、モール41は、受注番号を発番するとともに、第1署名付決済要求情報を発行する(④)。

【0123】

ユーザ2はモール41から送信された第1署名付決済要求情報およびカード情報(ID、残高等)をサイバー電子マネーシステム30に送信する(⑤)。

【0124】

サイバー電子マネーシステム30は、第1署名付決済要求情報を受けて、ユーザ2が所有するICカード20と通信を行い、第2署名付決済情報をICカード

20に送信し、ICカード20内に記憶されている価値情報から購入する商品またはサービスに対応する価値を減算し、カード内の履歴情報を吸い上げる(⑥)。

【0125】

サイバー電子マネーシステム30は、決済が完了した後に、第3署名付決済完了情報をモール71に送信する(⑦)。

【0126】

サイバー電子マネーシステム30は、決済が完了した後に、第3署名付決済完了情報をユーザ2に送信する(⑧)。

【0127】

第3署名付決済完了情報により決済が完了したことを確認した後に、ユーザ2は加盟店42に対して決済完了画面を要求する(⑨)。

【0128】

加盟店4は、ユーザ2からの決済完了画面要求に応じて、第4署名付決済完了受領情報をユーザ2およびサイバー電子マネーシステム30に送信するとともに、決済完了画面をユーザ2のパーソナルコンピュータ22に表示する(10)。

【0129】

以上の工程により決済が完了した後に、加盟店42からユーザ2に対して商品またはサービスが受け渡される。例えば、商品がデジタルコンテンツであるような場合には、加盟店42がユーザ2に対して、デジタルコンテンツのダウンロードを許可することにより、商品の受け渡しが行われる(11)。

【0130】

次に、図9～図11を参照しながら、共通鍵、公開鍵、および電子署名を用いた請求リティの高い本実施の形態にかかる電子決済システムにおける商品情報伝送シーケンスおよび価値情報伝送シーケンスについて、詳細に説明する。

【0131】

まず、図9示すユーザによる商品決定が行われる前に、ユーザ2がパーソナルコンピュータ22上で動作するブラウザプログラム23を用いて、ネットワーク5を介して、店舗装置4のネットワークサーバ40にアクセスを行う。当該アク

セスにより、ネットワーク 5 を介してネットワークサーバ 4 0 からパーソナルコンピュータ 2 2 に、店舗装置 4 が提供する商品情報が送信され、それに応じた画面がパーソナルコンピュータ 2 2 のディスプレイに表示される。

【 0 1 3 2 】

(第 1 実施形態) 以下、電子決済システム 1 の動作を図 9 ～図 1 1 各ステップ毎に説明する。なお、図 1 2 ～図 2 0 には、クライアント装置のパーソナルコンピュータ 2 2 の画面表示される例が示されている。

【 0 1 3 3 】

なお、以下に示す動作において、クライアント装置のパーソナルコンピュータ 2 2 とネットワークサーバ 4 0 との間で情報あるいは要求の送受信を行う際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において、当該秘密鍵に対応する公開鍵を用いて検証するが、当該処理については記載を省略する。

【 0 1 3 4 】

また、同様に、パーソナルコンピュータ 2 2 とアプリケーションサーバ 3 0 との間で情報あるいは要求の送受信を行う際に、送信元の秘密鍵を用いて作成した電子署名情報を、送信先において、当該秘密鍵に対応する公開鍵を用いて検証するが、当該処理についてはステップ S T 1 4 , S T 1 5 を除いて記載を省略する。

【 0 1 3 5 】

ステップ S T 1 :

パーソナルコンピュータ 2 2 とネットワークサーバ 4 0 との間で S S L (S e c u r e S o c k e t L a y e r) を用いた相互認証を行い、セキュアな通信路を確立する。

【 0 1 3 6 】

ステップ S T 2 :

ユーザ 2 が、図 1 2 に示すような商品選択画面において、パーソナルコンピュータ 2 2 のキーボードやマウスなどを操作して購入を希望する商品を決定すると、それに応じた商品決定情報がパーソナルコンピュータ 2 2 からネットワークサーバ 4 0 に送信される。

【0137】

ステップST3：

ネットワークサーバ40は、パーソナルコンピュータ22から商品決定情報を受けると、その見積もり情報をパーソナルコンピュータ22に送信する。

【0138】

ステップST4：

パーソナルコンピュータ22は、図13に示すように、ネットワークサーバ40から受けた見積もり情報をディスプレイに表示する。ユーザ2は、当該見積もりに同意した場合には、図14に示す画面において、支払い方法を選択する。ユーザ2が、パーソナルコンピュータ22のキーボードなどを操作して電子マネーを利用した決済を選択すると、請求額要求がネットワークサーバ40に送信される。

【0139】

ステップST5：

ネットワークサーバ40は、パーソナルコンピュータ22から請求額要求を受けると、店舗装置4がユーザ2に請求する金額を示す決済要求情報と、当該決済要求情報に対して店舗装置4の秘密鍵KSHOP,Sを用いて作成した第1署名情報SIG1と、インタフェースプログラム24とをパーソナルコンピュータ22に送信する。

【0140】

ステップST6：

パーソナルコンピュータ22は、図15に示すように、ステップST5でネットワークサーバ40から受信した決済要求情報が示す金額をディスプレイに表示する。

【0141】

ステップST7：

ステップST6でディスプレイに表示された金額に同意したユーザ2がパーソナルコンピュータ22のキーボードなどを用いて所定の指示を出すと、ステップST5でネットワークサーバ40から受信したインタフェースプログラム24が

起動される。

【0142】

そして、図16に示すような画面表示にしたがって、ユーザ2がICカード20をリーダライタ21にかざすと、パーソナルコンピュータ22は、起動されたインタフェースプログラム24を用いて、決済管理装置3のアプリケーションサーバ30との間でSSLを用いた相互認証を行い、セキュアな通信路を確立する。

【0143】

本実施の形態にかかる決済システムにおいて決済処理が行われている間は、パーソナルコンピュータ22のディスプレイには、図17に示すように、ユーザに待機を促すような画面が表示される。

【0144】

ステップST8：

パーソナルコンピュータ22は、ステップST5で店舗装置4のネットワークサーバ40から受信した決済要求情報と、当該決済要求情報に対する第1署名情報SIG1とを含む決済要求情報を決済管理装置3のアプリケーションサーバ30に送信する。

【0145】

ステップST9：

アプリケーションサーバ30は、例えば、情報管理サーバ32から読み出した店舗装置4に対応する公開鍵KSHOP,Pを用いて、ステップST8で受信した第1署名情報SIG1を検証し、当該第1署名情報SIG1が店舗装置4のネットワークサーバ40において付された正当なものであると判断すると、ステップST10の処理を行う。

【0146】

なお、アプリケーションサーバ30は、第1署名情報SIG1が不正なものであると判断した場合には、例えば、パーソナルコンピュータ22に対してのその旨を通知した後、処理を終了する。

【0147】

ステップ S T 1 0 :

次いで、決済管理装置 3 のアプリケーションサーバ 3 0 は、例えば、決済要求情報をセキュリティサーバ 3 1 に送信する。

【 0 1 4 8 】

ステップ S T 1 1 :

セキュリティサーバ 3 1 は、 I C カード 2 0 から決済要求情報を受けると、 I C カード 2 0 との間で相互認証を行い、 I C カード 2 0 との間で用いる共通鍵 K C からセッション鍵 K S E S を生成する。 I C カード 2 0 でも、同様に、共通鍵 K C からセッション鍵 K S E S を生成する。

【 0 1 4 9 】

ステップ S T 1 2 :

セキュリティサーバ 3 1 は、決済情報を生成し、これをセッション鍵 K S E S で暗号化してアプリケーションサーバ 3 0 に出力する。その際に、セキュリティサーバ 3 1 は、決済管理装置の秘密鍵を用いて作成した第 2 署名を付す。

【 0 1 5 0 】

アプリケーションサーバ 3 0 は、セキュリティサーバ 3 1 から入力した残高読み出し要求 (B R C) を含む決済情報をパーソナルコンピュータ 2 2 に送信する。

【 0 1 5 1 】

パーソナルコンピュータ 2 2 は、アプリケーションサーバ 3 0 から受信した残高読み出し要求 B R C を含む決済情報をリーダーライタ 2 1 を介して I C カード 2 0 に出力する。

【 0 1 5 2 】

ステップ S T 1 3 :

I C カード 2 0 は、パーソナルコンピュータ 2 2 からの残高読み出し要求 B R C を含む決済情報が入力されると、これをステップ S T 1 1 で生成したセッション鍵 K S E S を用いて復号する。

【 0 1 5 3 】

そして、 I C カード 2 0 は、残高読み出し要求 B R C を含む決済情報に応じた

処理回路51の処理によって、ICカード20内の耐タンパ性のメモリ52から残高情報BIを含む決済情報を読み出し、これをセッション鍵KSESを用いて暗号化した後に、パーソナルコンピュータ22に出力する。

【0154】

パーソナルコンピュータ22は、ICカード20からの残高情報BIを含む決済情報をアプリケーションサーバ30に送信する。

【0155】

アプリケーションサーバ30は、パーソナルコンピュータ22から受信した残高情報BIを決済情報をセキュリティサーバ31に出力する。

【0156】

セキュリティサーバ31は、アプリケーションサーバ30から入力した残高情報BIを含む決済情報をセッション鍵KSESを用いて復号し、ログ情報を生成する。

【0157】

ステップST14：

セキュリティサーバ31は、ステップST13で生成したログ情報をICカード20に書き込むためのログ書き込み情報と、ICカード20に記憶された残高情報が示す金額から請求額を減算するための減算額を示す減算情報とを含む決済処理要求SPCを生成し、これをセッション鍵KSESを用いて暗号化する。

【0158】

次に、セキュリティサーバ31は、平文の残高情報BIと、暗号化された決済処理要求SPCとを含む決済情報をアプリケーションサーバ30に出力する。

【0159】

アプリケーションサーバ30は、セキュリティサーバ31から入力した残高情報BIおよび決済処理要求SPCを含む決済情報に対する第2署名情報をアプリケーションサーバ30の秘密鍵を用いて作成する。

【0160】

次に、アプリケーションサーバ30は、セキュリティサーバ31から入力した残高情報BIおよび決済処理要求SPCを含む決済情報に対して第2署名情報を

付してパーソナルコンピュータ 2 2 に送信する。

【 0 1 6 1 】

ステップ S T 1 5 :

パーソナルコンピュータ 2 2 は、アプリケーションサーバ 3 0 から受信した第 2 署名情報 S I G 2 の正当性を、アプリケーションサーバ 3 0 の公開鍵を用いて検証し、その正当性が認められた後に、以下に示す処理を行う。

【 0 1 6 2 】

パーソナルコンピュータ 2 2 は、図 1 8 に示すように、アプリケーションサーバ 3 0 から受信した残高情報 B I が示す残高、並びにステップ S T 3 でネットワークサーバ 4 0 から受信した見積もり情報が示す金額（請求額）をディスプレイに表示する。

【 0 1 6 3 】

ステップ S T 1 6 :

パーソナルコンピュータ 2 2 は、ステップ S T 1 5 でディスプレイに表示された残高および請求額に同意したユーザ 2 がパーソナルコンピュータ 2 2 のキーボードなどを用いて所定の指示を出すと、決済処理要求 S P C を I C カードリーダー 2 1 を介して I C カード 2 0 に出力する。支払確認処理が行われている間は、図 1 9 に示すような待機を促す画面がパーソナルコンピュータ 2 2 のディスプレイに表示される。

【 0 1 6 4 】

ステップ S T 1 7 :

I C カード 2 0 は、パーソナルコンピュータ 2 2 から入力した決済処理要求 S P C をセッション鍵 K S E S を用いて復号し、当該決済処理要求に応じた決済処理を処理回路 5 1 で実行する。

【 0 1 6 5 】

具体的には、I C カード 2 0 は、処理回路 5 1 の処理によって、決済処理要求 S P C に含まれるログ書き込み情報を、I C カード 2 0 内の耐タンパ性のメモリ 5 2 に記憶する。また、I C カード 2 0 は、処理回路 5 1 の処理によって、メモリ 5 2 に記憶されている残高情報が示す残高から、決済処理要求 S P C に含まれ

る減算情報が示す減算額を減算し、その結果を残高情報としてメモリ52に記憶する。

【0166】

ステップST18:

ICカード20は、ステップST17の処理が完了すると、処理が完了したことを示す処理完了通知PCNを生成し、これをセッション鍵KSESで暗号化した後に、パーソナルコンピュータ22およびアプリケーションサーバ30を介して、セキュリティサーバ31に送信する。

【0167】

ステップST19:

セキュリティサーバ31は、ICカード20からの処理完了通知PCNを受信すると、これをセッション鍵KSESを用いて復号し、処理完了通知PCNを確認した後に、決済完了情報ACNを生成し、これをアプリケーションサーバ30を介してパーソナルコンピュータ22およびネットワークサーバ40に送信する。その際に、決済完了情報は、決済管理装置が生成する第3署名を付することにより、その正当性が確保される。

【0168】

ステップST20:

パーソナルコンピュータ22は、セキュリティサーバ31からの決済完了通知ACNを受信すると、図20に示すように、これに応じた情報、例えばデジタルコンテンツのダウンロードを促すような画面をディスプレイに表示する。

【0169】

以上説明したように、電子決済システム1によれば、ICカード20のメモリ52に共通鍵KCを記憶し、秘密鍵は記憶しない。そのため、ユーザ2がICカード20を紛失した場合でも、メモリ52には秘密鍵が記憶されていないため、秘密鍵を用いてユーザ2の署名が不正に行われることを回避できる。

【0170】

また、電子決済システム1によれば、共通鍵KCはICカード20およびセキュリティサーバ31の内部でのみ使用されることから、共通鍵KCが盗まれる危

険性を低くでき、安全な取り引きを実現できると共に、鍵管理を容易にすることができる。

【0171】

また、電子決済システム1によれば、ICカード20に入出力される情報および要求をパーソナルコンピュータ22を介して行い、パーソナルコンピュータ22と、アプリケーションサーバ30およびネットワークサーバ40との間で情報および要求を送受信する際に、秘密鍵および公開鍵を用いた署名検証を行うことから、当該情報および要求がネットワーク5上で不正に改竄されることを回避でき、ネットワーク5を用いた取り引きの安全性を確保できる。

【0172】

また、電子決済システム1によれば、店舗装置4のネットワークサーバ40において、請求額情報BILLに対して自らの秘密鍵KSHOP,Sを用いて作成した署名情報SIGを付し、決済管理装置3のアプリケーションサーバ30において、秘密鍵KSHOP,Sに対応する公開鍵KSHOP,Pを用いて署名情報SIGを検証し、当該署名情報SIGが店舗装置4のネットワークサーバ40において付された正当なものであると判断することから、ユーザ2のパーソナルコンピュータ22などにおいて、不正に改竄された請求額情報BILLに基づいて決済が行われてしまうことを防止できる。

【0173】

また、電子決済システム1では、前述したように、パーソナルコンピュータ22は、アプリケーションサーバ30から受信した残高情報BIが示す残高、並びにネットワークサーバ40から受信した見積もり情報が示す金額（請求額）をディスプレイに表示し、その内容にユーザ2が同意した後に、アプリケーションサーバ30から受信した決済処理要求SPCをICカードリーダライタ21を介してICカード20に出力する。従って、ユーザ2は、ICカード20内で最終的に行われる決済処理の内容を事前に確認でき、不正に改竄された内容で決済処理が行われることを防止できる。

【0174】

また、電子決済システム1によれば、決済処理に伴う手順を従来に比べて少な

くでき、ネットワーク5を介した情報伝送を削減でき、ネットワーク5の利用量の削減、並びに処理時間を短縮を図れる。

【0175】

また、電子決済システム1によれば、従来のSET方式のように、署名情報の作成および検証を多数回行う必要がない。

【0176】

(第2実施形態)

次に図21～図23を参照しながら、別の実施の形態にかかる決済システムによる商品情報伝送シーケンスおよび価値情報伝送シーケンスについて説明する。

【0177】

ST101:

まず、ユーザ2のパーソナルコンピュータ22と店舗装置4のネットワークサーバ40との間においてセキュリティにすぐれた通信のためにSSL認証が確立される。

【0178】

ST102:

次いで、ユーザ2は、パーソナルコンピュータ22のディスプレイに表示される画面に応じて、商品の選択を行う。

【0179】

ST103:

店舗装置4のネットワークサーバ40は、ユーザ2が選択した商品に応じて、店舗装置4の秘密鍵を用いて作成された第1署名が付された決済処理要求情報を、ユーザ2のパーソナルコンピュータ22に送信する。

【0180】

ST104:

パーソナルコンピュータ22は、ActiveXなどのインタフェースプログラム24を起動して、リーダライタ21を介してICカード20にアクセスし、ICカードの残高を読み出す。

【0181】

ST105:

読み出された残高は、所定のブラウジング機構を利用して、ユーザ2のパーソナルコンピュータ22に取り込まれ、ディスプレイ上に表示される。

【0182】

ST106:

次いで、ユーザ2のパーソナルコンピュータ22と決済管理装置3のアプリケーションサーバ30との間にセキュアなSSL認証を確立し、価値情報伝送シーケンスに備える。

【0183】

ST107:

次いで、ユーザ2のパーソナルコンピュータ22からICカード20の残高情報を含む第1署名付の決済要求情報が決済管理装置3に送信される。

【0184】

決済管理装置3のアプリケーションサーバ30は、店舗装置4の秘密鍵に対応する公開鍵により、送信された決済要求情報の正当性を検証し、必要な情報をセキュリティサーバ31に受け渡す。

【0185】

ST108:

決済管理装置3のセキュリティサーバ31は、ICカード20との間で相互認証を行い、共通鍵からセッション鍵を生成する。同様に、ICカード20側においても、セキュリティサーバ31との間で相互認証を行い、共通鍵からセッション鍵を生成する。

【0186】

ST109:

セキュリティサーバ31は、決済情報をセッション鍵で暗号化し、アプリケーションサーバ30を介してユーザ2のパーソナルコンピュータ22に送信する。

【0187】

パーソナルコンピュータ22では、送られてきた決済情報を、ICカード20が記憶しているセッション鍵で復号化して画面表示する。ユーザ2が送られてき

た決済情報を承認する場合には、リーダライタ21を介して、その内容がICカード20に送信され、ICカード20内において、減算処理などの所定の決算処理が行われる。

【0188】

なお、ここで留意すべきは、本実施形態にかかる決算シーケンスにおいては、図9～図11に関連して説明した決算シーケンスとは異なり、決算管理装置3のセキュリティサーバ31により生成される決算情報は、単に共通鍵により暗号化されるのみで、決算管理装置3が有する秘密鍵を用いて生成される第2署名が付されない点である。

【0189】

このように、単に共通鍵による暗号化／復号化によっても、送信される決算情報の身元は確認可能なので、本実施の形態にかかる決算システムのように、第2署名を省略することにより、処理の冗長性を緩和することが可能である。

【0190】

ST110:

以上説明したようにして、ICカード20内において、所定の決算処理が終了すると、その結果が、リーダライタ21、パーソナルコンピュータ22、アプリケーションサーバ30を介してセキュリティサーバ31に送信される。

【0191】

ST111:

セキュリティサーバ31により決算完了が確認されると、その決算完了情報がアプリケーションサーバ30に送られる。そして、決算完了情報（領収書）は、アプリケーションサーバ31において、決算管理装置3の秘密鍵を用いて生成された第3署名が付されて、店舗装置2のネットワークサーバ40に送信される。

【0192】

ST112:

ネットワークサーバ40においては、決算管理装置3の秘密鍵に対応する公開鍵により決算完了情報を検証し、その内容を確認後、決済完了受領情報を生成する。この決済完了受領情報は、店舗装置4の秘密鍵を用いて生成された第4署名

が付されて、決算管理装置 3 のアプリケーションサーバ 3 0 に送信される。

【 0 1 9 3 】

そして、決算管理装置 3 のアプリケーションサーバ 3 0 が、第 4 署名付決済完了受領情報を、ユーザ 2 のパーソナルコンピュータ 2 2 に送信することにより、パーソナルコンピュータ 2 2 のディスプレイには、一連の電子マネー決済処理が完了した旨の表示が成される。

【 0 1 9 4 】

以上説明したように、本実施の形態にかかる電子決済システムによれば、IC カード 2 0 のメモリ 5 2 に共通鍵を記憶し、秘密鍵は記憶しない。そのため、ユーザ 2 が IC カード 2 0 を紛失した場合でも、メモリ 5 2 には秘密鍵が記憶されていないため、秘密鍵を用いてユーザ 2 の署名が不正に行われることを回避できる。

【 0 1 9 5 】

また、本実施の形態にかかる電子決済システムによれば、共通鍵は IC カード 2 0 およびセキュリティサーバ 3 1 の内部でのみ使用されることから、共通鍵が盗まれる危険性を低くでき、安全な取引を実現できると共に、鍵管理を容易にすることができる。

【 0 1 9 6 】

また、本実施の形態にかかる電子決済システムによれば、IC カード 2 0 に入出力される情報および要求をパーソナルコンピュータ 2 2 を介して行い、パーソナルコンピュータ 2 2 と、アプリケーションサーバ 3 0 およびネットワークサーバ 4 0 との間で情報および要求を送受信する際に、秘密鍵および公開鍵を用いた署名検証を行うことから、当該情報および要求がネットワーク 5 上で不正に改竄されることを回避でき、ネットワーク 5 を用いた取引の安全性を確保できる。

【 0 1 9 7 】

なお署名検証を行わない場合であっても、共通鍵による暗号化／復号化によって、送信される決算情報の身元は確認可能なので、本実施の形態にかかる決算システムのように、処理の冗長性を緩和することが可能である。

【 0 1 9 8 】

また、本実施の形態にかかる電子決済システムによれば、店舗装置 4 のネットワークサーバ 4 0 において、決済要求情報に対して自らの秘密鍵を用いて作成した第 1 署名情報を付し、決済管理装置 3 のアプリケーションサーバ 3 0 において、秘密鍵に対応する公開鍵を用いて第 1 署名情報を検証し、当該第 1 署名情報が店舗装置 4 のネットワークサーバ 4 0 において付された正当なものであると判断することから、ユーザ 2 のパーソナルコンピュータ 2 2 などにおいて、不正に改竄された決済要求情報に基づいて決済が行われてしまうことを防止できる。

【 0 1 9 9 】

また、本実施の形態にかかる電子決済システムでは、前述したように、パーソナルコンピュータ 2 2 は、アプリケーションサーバ 3 0 から受信した残高情報が示す残高、並びにネットワークサーバ 4 0 から受信した見積もり情報が示す金額（請求額）をディスプレイに表示し、その内容にユーザ 2 が同意した後に、アプリケーションサーバ 3 0 から受信した決済処理要求 S P C を I C カードリーダー 2 1 を介して I C カード 2 0 に出力する。従って、ユーザ 2 は、I C カード 2 0 内で最終的に行われる決済処理の内容を事前に確認でき、不正に改竄された内容で決済処理が行われることを防止できる。

【 0 2 0 0 】

また、電子決済システム 1 によれば、決済処理に伴う手順を従来に比べて少なくでき、ネットワーク 5 を介した情報伝送を削減でき、ネットワーク 5 の利用量の削減、並びに処理時間を短縮を図れる。

【 0 2 0 1 】

また、電子決済システム 1 によれば、従来の S E T 方式のように、署名情報の作成および検証を多数回行う必要がないがため、処理手順の冗長性を緩和できる。

【 0 2 0 2 】

（電子マネー入金システム）

図 2 4 ～ 図 3 1 を参照しながら、本実施の形態にかかる決済システムにおける電子マネー入金システムおよびシーケンスについて説明することにする。

【0203】

本実施の形態にかかる決済システムにおいては、プリペイド方式の電子マネーとしてICカード20を利用するのであるが、ユーザ2はICカード20に記憶された価値情報の残高が不足した場合には、その残高を増やすように、価値情報の更新を行う必要がある。あるいは、場合によっては、ICカード20に記憶された価値情報を減額するように、価値情報の更新を行う必要がある。

【0204】

電子マネーをICカードに入金する際には、ユーザ2は、リーダライタ21によりICカード20にアクセス可能なパーソナルコンピュータ20を介して決済管理装置3のアプリケーションサーバ（サイバー電子マネーシステム）30にアクセスし、入金画面をディスプレイ上に表示するように要求する（①）。

【0205】

かかる入金画面要求を受けて、アプリケーションサーバ30は、Active Xコンポーネントなどの所定のインタフェースプログラム24を介して、ユーザ2のパーソナルコンピュータ20のディスプレイに、図25に示すような入金画面が表示される（②）。

【0206】

ユーザ2が図25に示す入金画面において、入金を選択すると、図26に示すように、ICカード20をリーダライタ21にセットするように指示がだされる。

【0207】

ユーザ2が、ICカード20をリーダライタ21にセットすると、ICカード20内に記憶されている残高などが読み出され、サイバー電子マネーシステム30に転送される（③）。また、同時に、カード内の履歴情報などもサイバー電子マネーシステムに吸い上げられる（④）。これらの処理が行われている間は、図27に示すように、処理中である旨の表示がディスプレイに表示される。

【0208】

次いで、ユーザ2が、図28および図29に示されるような画面を参照しながら、パーソナルコンピュータ22のキーボードやマウスなどを操作しながら、入

金金額、クレジットカードの番号や有効期限や暗証番号を入力してサイバー電子マネーシステムに転送する(③)。また、同時に、カード内の履歴情報などもサイバー電子マネーシステムに吸い上げられる(④)。これらの処理が行われている間は、図30に示すように、処理中である旨の表示がディスプレイに表示される。

【0209】

サイバー電子マネーシステム30は、上記のような入金要求情報を受けると、与信装置35に対して、クレジット決済要求の承認を求める(⑤)。与信装置35は、クレジット情報を精査した後、クレジット決済要求の可否を決定する。なお与信装置35の詳細な構成については、本発明とは直接的な関係を有しないので、詳細な説明は省略することにする。

【0210】

与信の結果が肯定的である場合には、サイバー電子マネーシステムは、価値更新情報を生成する。サイバー電子マネーシステムは、価値更新情報を、決済管理装置3とICカード20との間で共用される共通鍵により暗号化する。

【0211】

さらに、価値更新情報は、決済管理装置3の秘密鍵により作成される第5署名を付されて、ユーザ2のパーソナルコンピュータ22に送信される。ユーザ2のパーソナルコンピュータ22は、決済管理装置3の秘密鍵に対応する公開鍵により、送られてきた価値更新情報の正当性を検証し、正しいものであれば、その価値更新情報を決済管理装置3とICカード20との間で共用される共通鍵により復号化する。そして、復号化された価値更新情報に基づいてICカード20内の価値情報を更新する(⑥)。

【0212】

パーソナルコンピュータ22は、サイバー電子マネーシステム30に対して入金完了画面要求を送信し(⑦)、図31に示すような、入金完了画面がパーソナルコンピュータ22のディスプレイに表示される(⑧)。その後、図32に示すように、サイバー電子マネーシステムのトップページに復帰して、一連の価値更新処理が完了する。

【0213】

なお、一連の処理に関するカードログ情報は、バッチ処理で、精査・決済システム用の情報管理サーバ32に送られて、保存される。

【0214】

以上説明したように、本実施の形態にかかる決済システムを利用した電子マネー入金システムによれば、ICカード20のメモリ52に共通鍵KCを記憶し、秘密鍵は記憶しない。そのため、ユーザ2がICカード20を紛失した場合でも、メモリ52には秘密鍵が記憶されていないため、秘密鍵を用いてユーザ2の署名が不正に行われることを回避できる。

【0215】

また、電子決済システム1によれば、共通鍵はICカード20およびセキュリティサーバ31の内部でのみ使用されることから、共通鍵が盗まれる危険性を低くでき、安全な入金処理を実現できると共に、鍵管理を容易にすることができる。

【0216】

以上、添付図面を参照しながら本発明にかかる電子決済システム等の好適な実施形態について説明したが、本発明はかかる例に限定されない。当業者であれば、特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【0217】

例えば、上述した実施形態では、図1に示すように、決済管理装置3において、アプリケーションサーバ30、セキュリティサーバ31および情報管理サーバ32を別々に設けた場合を例示したが、これらのサーバの機能を一つのサーバで実現してもよい。

【0218】

また、上述した実施形態では、ICカード20内の残高情報をアプリケーションサーバ30に読み出す場合を例示したが、当該残高情報をアプリケーションサーバ30に読み出さないようにしてもよい。

【0219】

【発明の効果】 以上説明したように、本発明によれば、共通鍵を保持したICカードを用いて、ネットワークを介した電子商取引を安全に行う電子決済システム、決済管理装置、店舗装置、クライアント装置、ICカード、コンピュータプログラムおよび記憶媒体を提供できる。

【0220】

特に、本発明にかかる電子決済システム等によれば、ICカード20のメモリ52に共通鍵を記憶し、秘密鍵は記憶しない。そのため、ユーザがICカードを紛失した場合でも、メモリには秘密鍵が記憶されていないため、秘密鍵を用いてユーザの署名が不正に行われることを回避できる。

【0221】

また、本発明にかかる電子決済システム等によれば、共通鍵はICカードおよびセキュリティサーバの内部でのみ使用されることから、共通鍵が盗まれる危険性を低くでき、安全な取引を実現できると共に、鍵管理を容易にすることができる。

【0222】

また、本発明にかかる電子決済システム等によれば、ネットワークを流通する各種情報および要求を送受信する際に、秘密鍵および公開鍵を用いた署名検証を行うことから、当該情報および要求がネットワーク上で不正に改竄されることを回避でき、ネットワークを用いた取引の安全性を確保できる。

【0223】

このように、本発明にかかる電子決済システム等によれば、決済処理や入金処理に伴う手順を従来に比べて少なくでき、ネットワークを介した情報伝送を削減でき、ネットワークの利用量の削減、並びに処理時間を短縮を図れる。

【図面の簡単な説明】

【図1】 図1は、本発明の一実施形態にかかる電子決済システムの全体構成図である。

【図2】 図2は、図1に示すICカードの構成を説明するための概略的な説明図である。

【図 3】 図 3 は、本発明の実施形態にかかる電子決済システムの別の構成例を示す構成図である。

【図 4】 図 4 は、本発明の実施形態にかかる電子決済システムにおける情報の流れを示す構成図である。

【図 5】 ユーザの IC カードと、決済管理装置のセキュリティサーバとの間の通信方法を説明するための図である。

【図 6】 ユーザのパーソナルコンピュータと、店舗のネットワークサーバとの間の通信方法を説明するための図である。

【図 7】 ユーザのパーソナルコンピュータと、決済管理装置のアプリケーションサーバとの間の通信方法を説明するための図である。

【図 8】 本発明の実施形態にかかる電子決済システムの電子マネー出金の流れを示す説明図である。

【図 9】 図 1 に示す電子決済システムの動作を説明するための図であり、商品情報伝送シーケンスを示している。

【図 1 0】 図 1 に示す電子決済システムの動作を説明するための図であり、価値情報伝送シーケンスを示している。

【図 1 1】 図 1 に示す電子決済システムの動作を説明するための図であり、価値情報伝送シーケンスを示している。

【図 1 2】 図 1 に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図 1 3】 図 1 に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図 1 4】 図 1 に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図 1 5】 図 1 に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図 1 6】 図 1 に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図 1 7】 図 1 に示す電子決済システムの決済動作中にクライアント装置

に表示される画面構成例である。

【図 1 8】 図 1 に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図 1 9】 図 1 に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図 2 0】 図 1 に示す電子決済システムの決済動作中にクライアント装置に表示される画面構成例である。

【図 2 1】 図 1 に示す電子決済システムの動作を説明するための図であり、商品情報伝送シーケンスを示している。

【図 2 2】 図 1 に示す電子決済システムの動作を説明するための図であり、価値情報伝送シーケンスを示している。

【図 2 3】 図 1 に示す電子決済システムの動作を説明するための図であり、価値情報伝送シーケンスを示している。

【図 2 4】 本発明の実施形態にかかる電子決済システムの電子マネー入金の流れを示す説明図である。

【図 2 5】 図 1 に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図 2 6】 図 1 に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図 2 7】 図 1 に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図 2 8】 図 1 に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図 2 9】 図 1 に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図 3 0】 図 1 に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

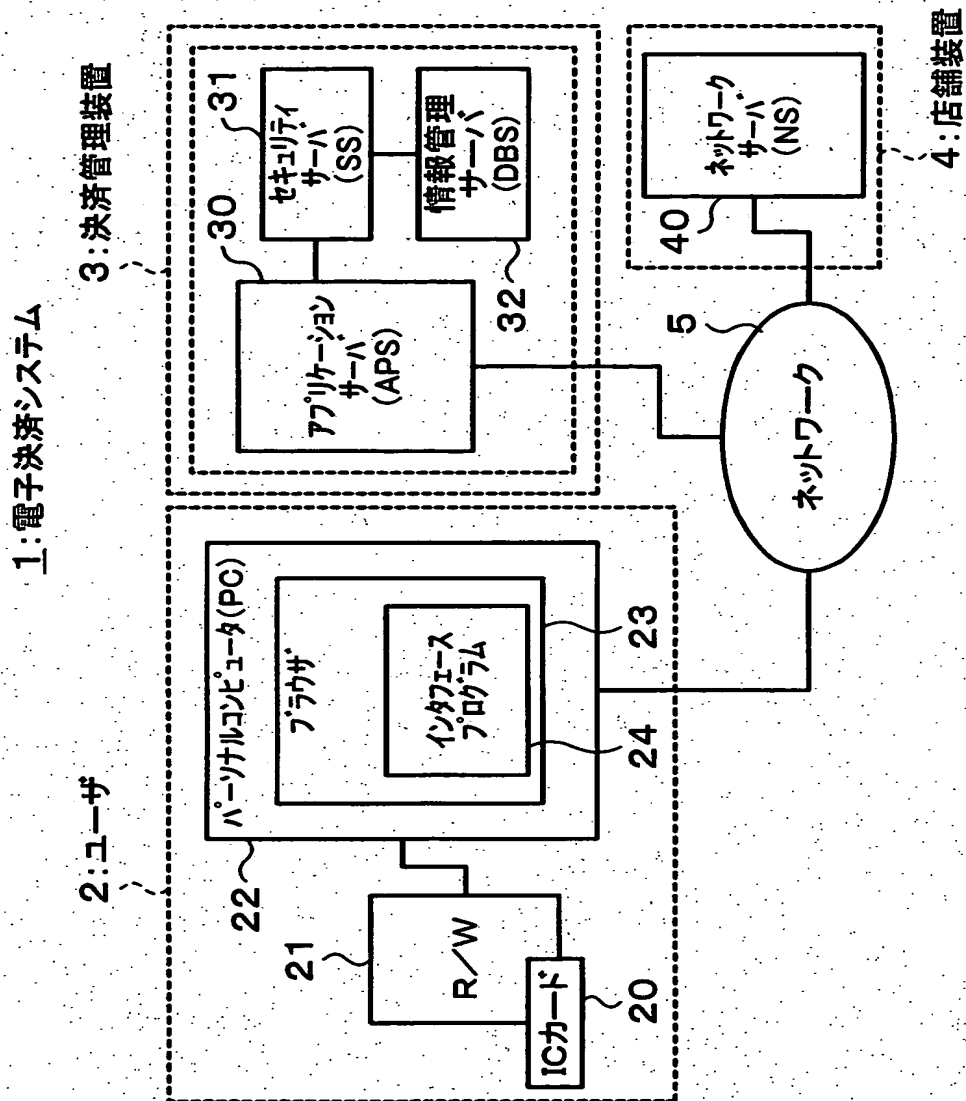
【図 3 1】 図 1 に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

【図 3 2】 図 1 に示す電子決済システムの入金動作中にクライアント装置に表示される画面構成例である。

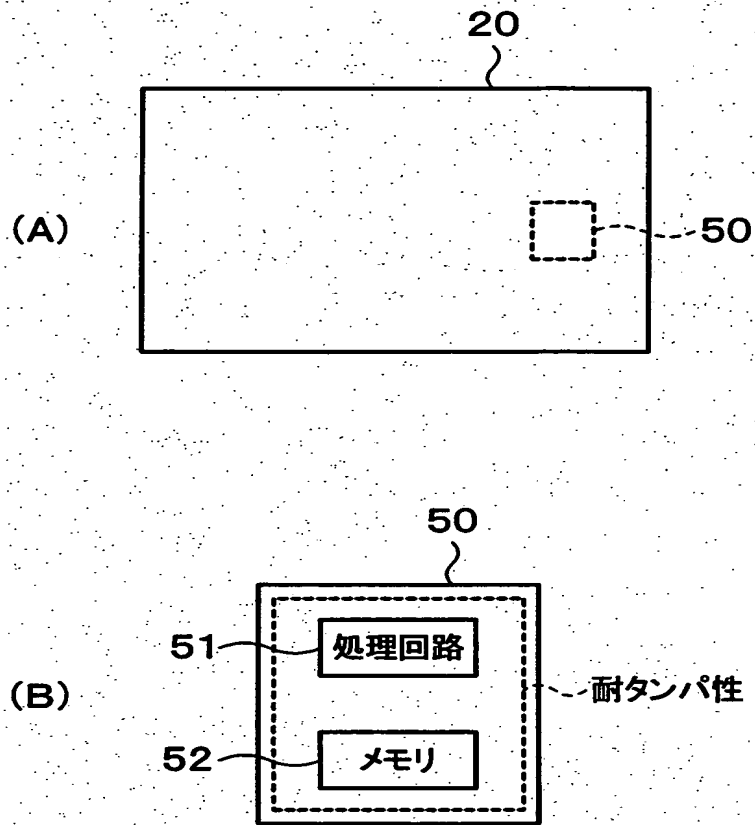
【符号の説明】 1 …電子決済システム,
2 …ユーザ,
3 …決済管理装置,
4 …店舗装置,
5 …ネットワーク,
2 0 … I C カード,
2 1 … I C カードリーダライタ,
2 2 …パーソナルコンピュータ,
2 3 …ブラウザプログラム,
2 4 …インタフェースプログラム,
3 0 …アプリケーションサーバ,
3 1 …セキュリティサーバ,
3 2 …情報管理サーバ,
4 0 …ネットワークサーバ

【書類名】 図面

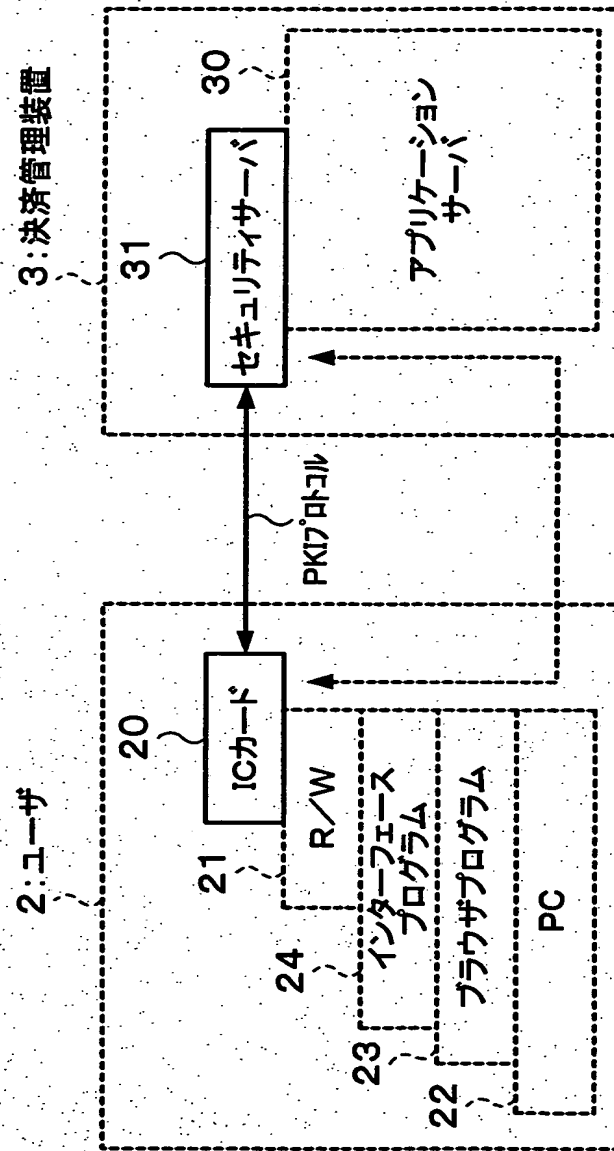
【図 1】



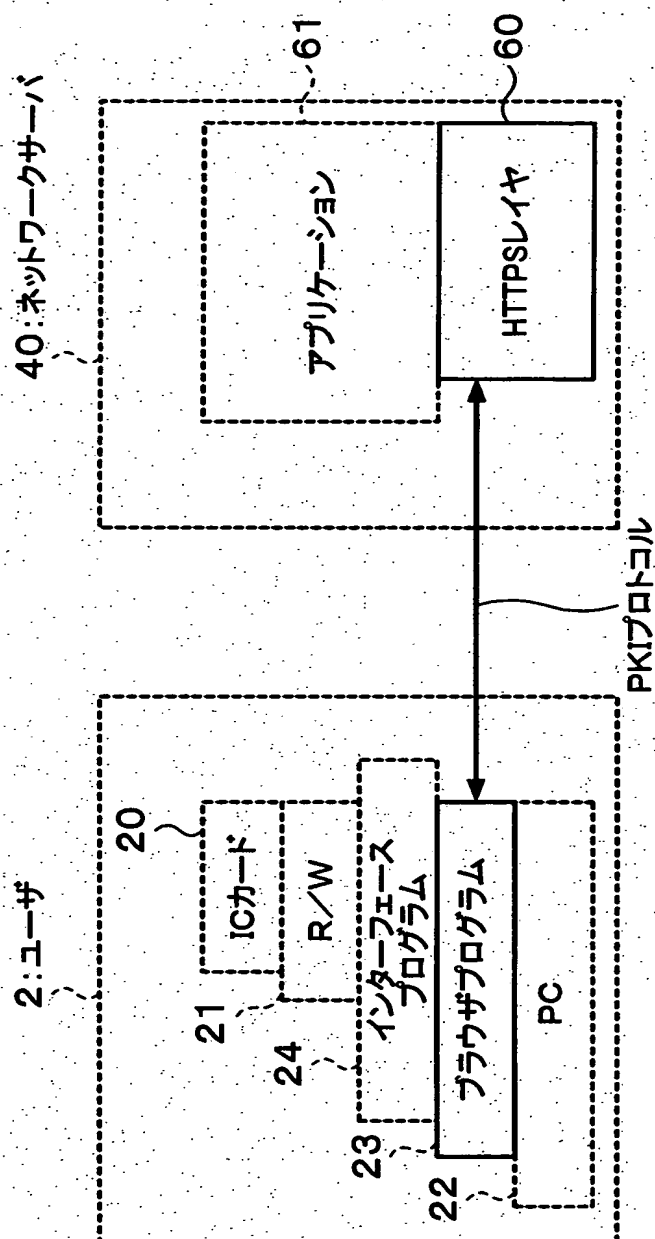
【図 2】



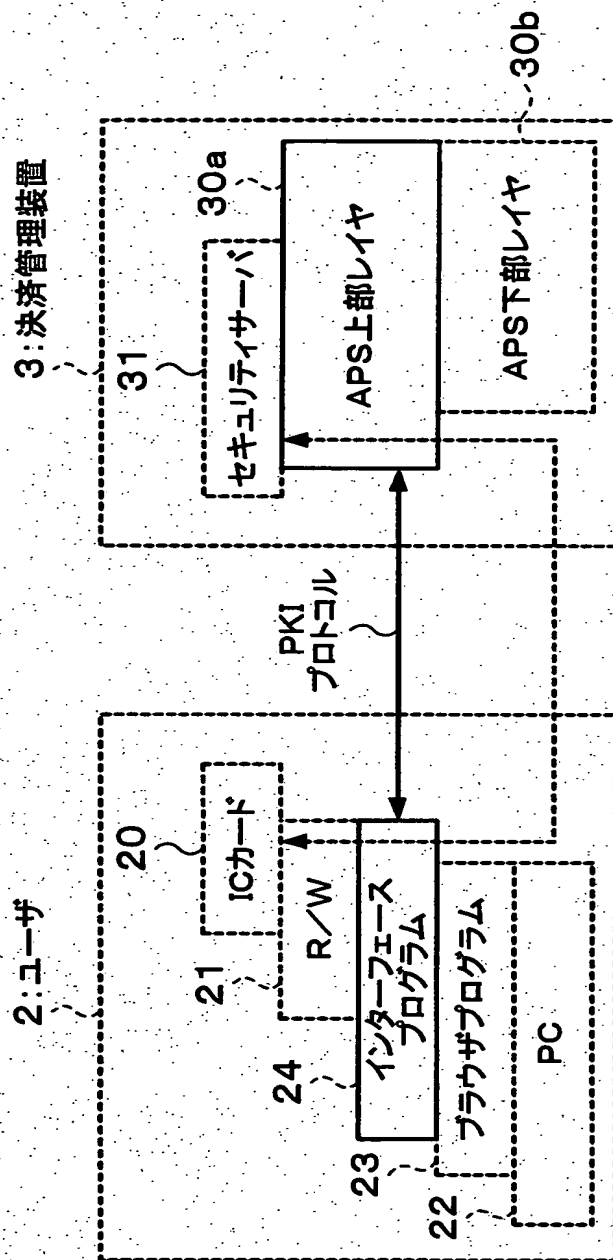
【図3】



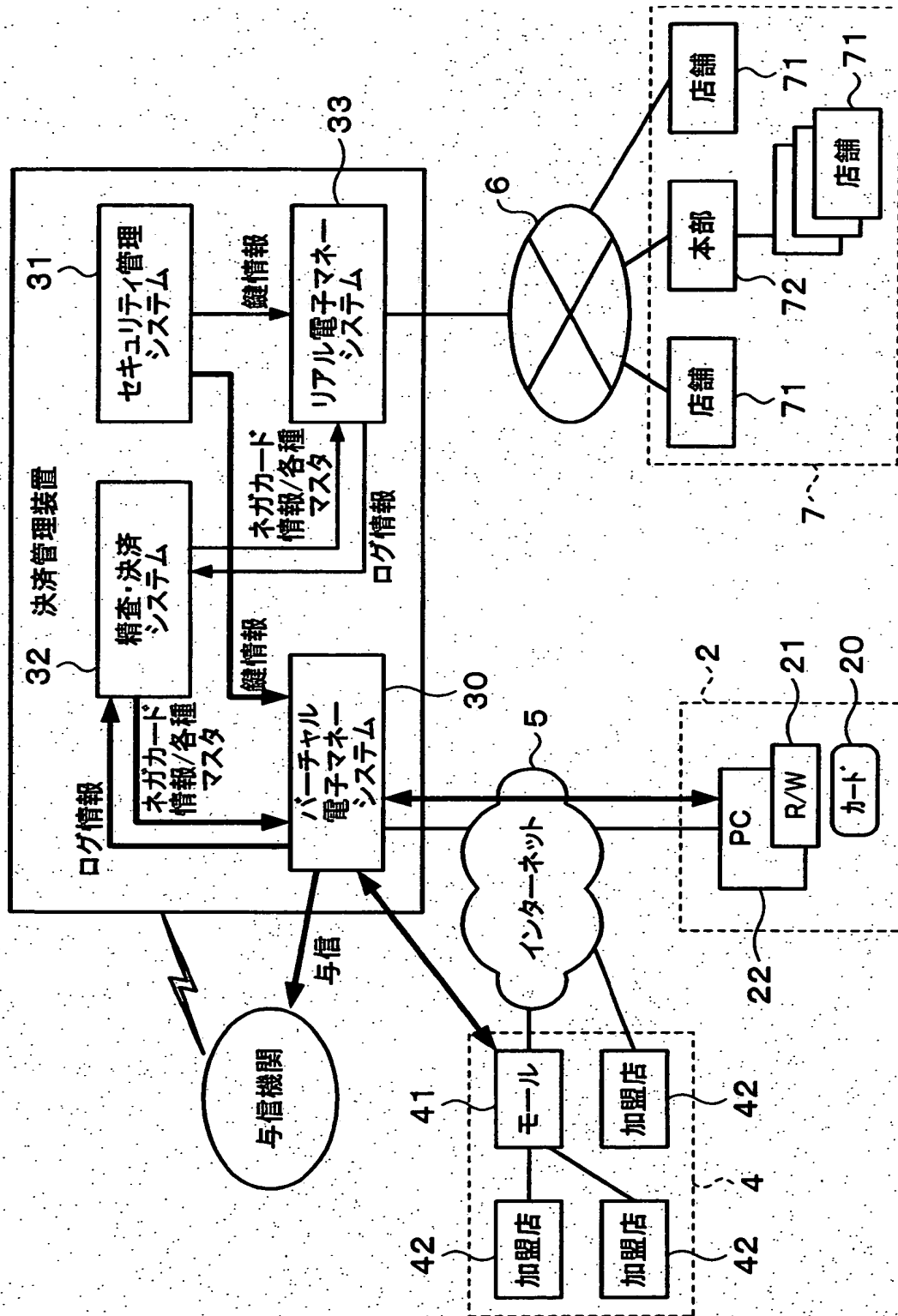
【図4】



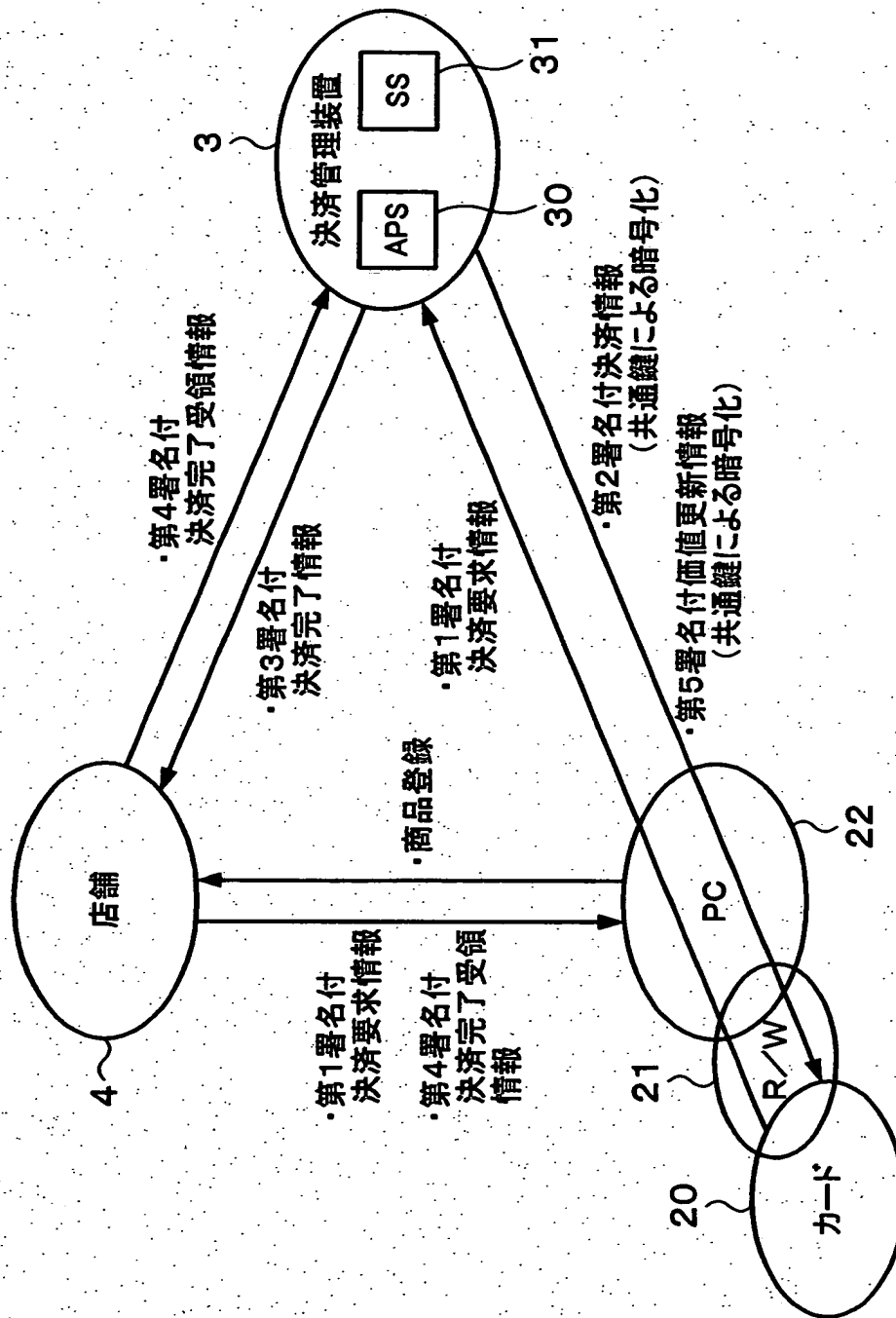
【図 5】



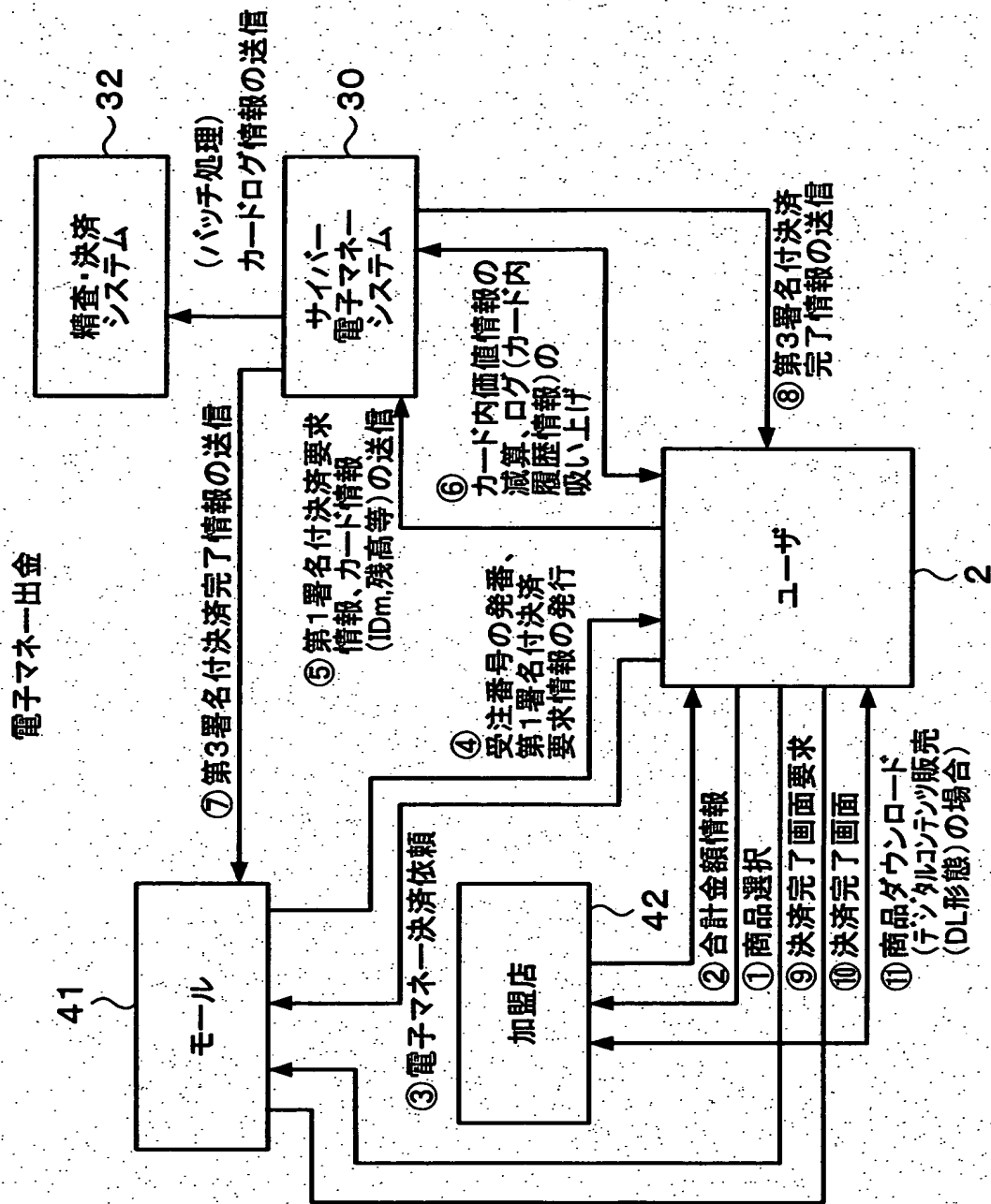
【図6】



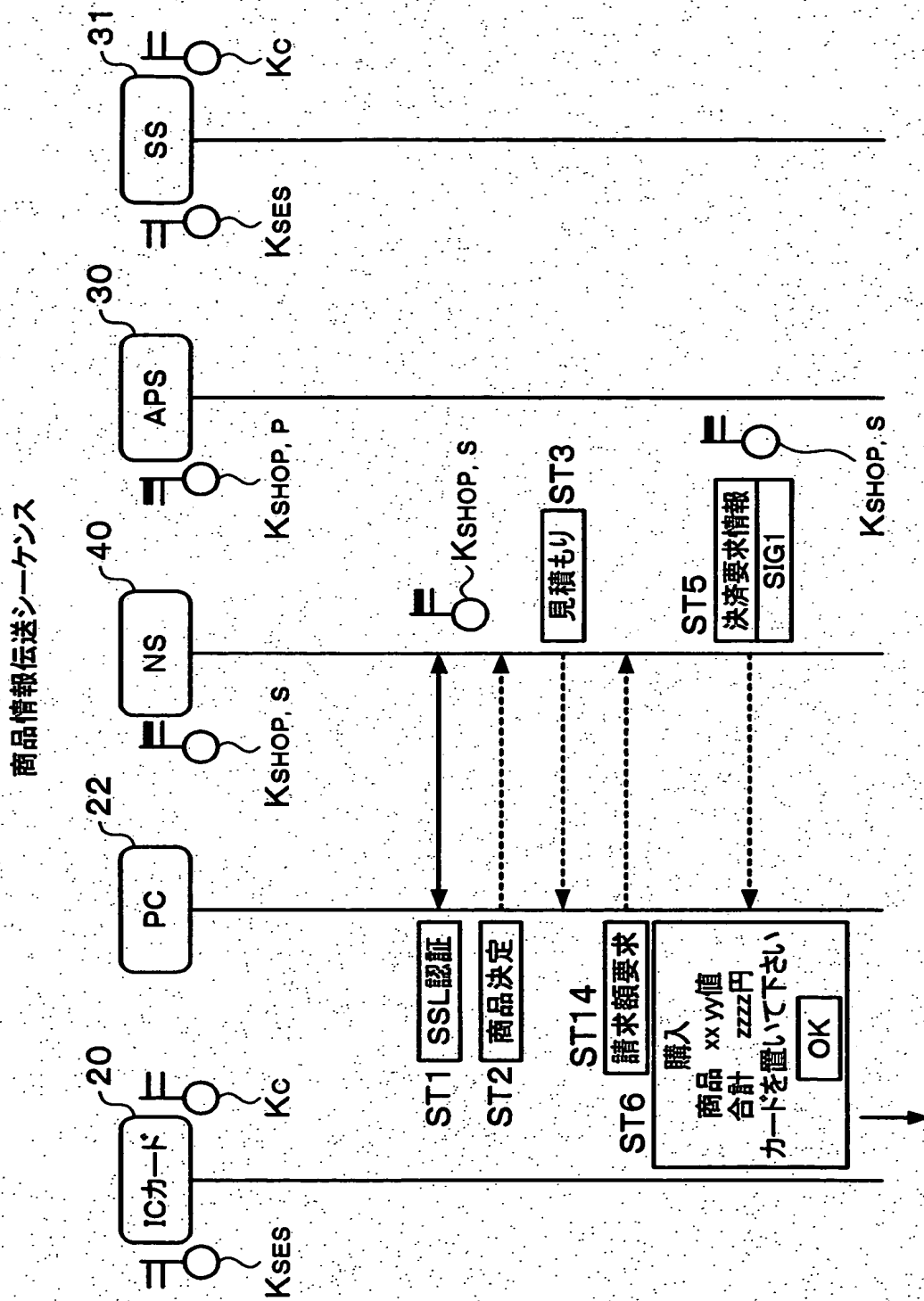
【図 7】



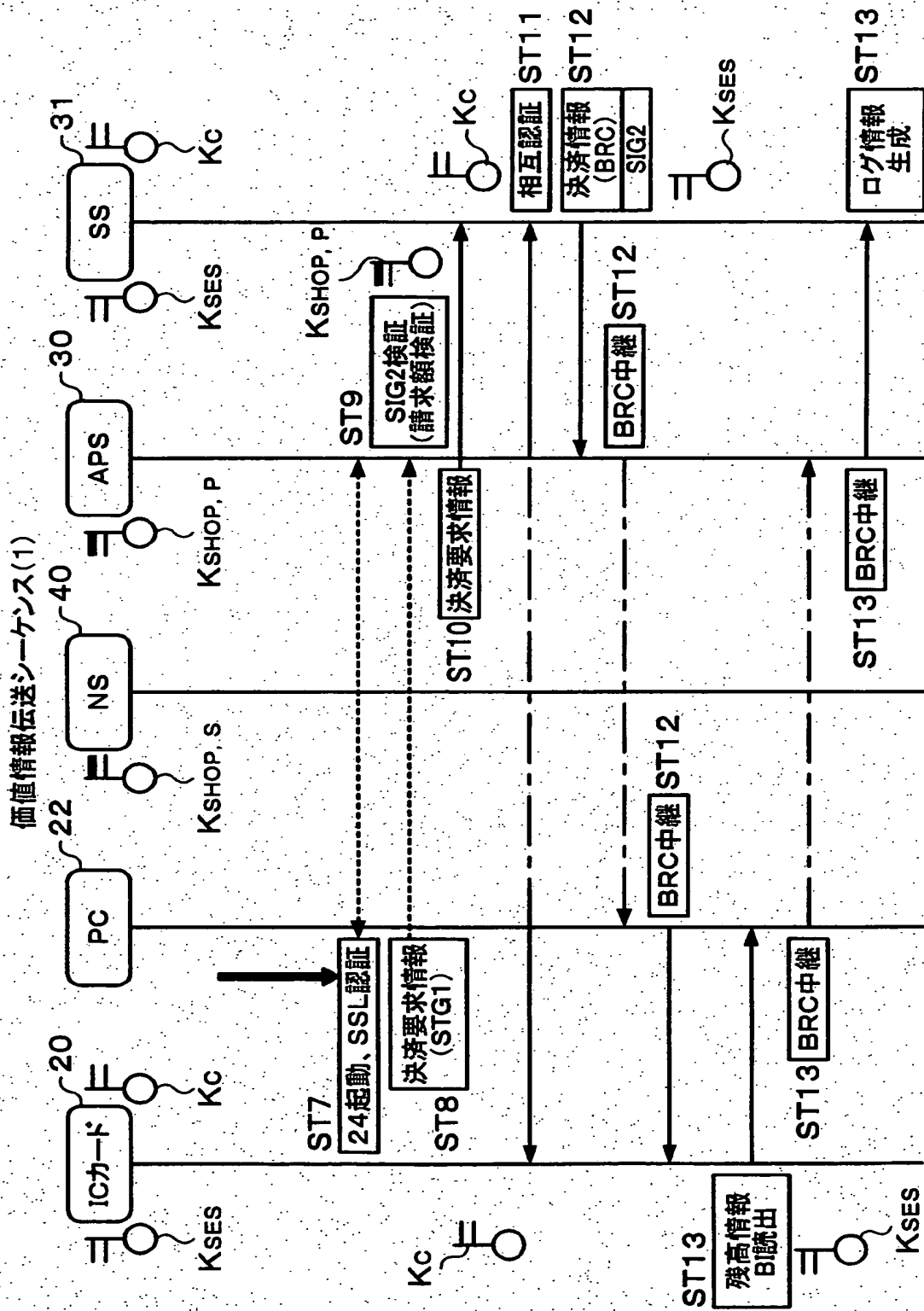
【図 8】



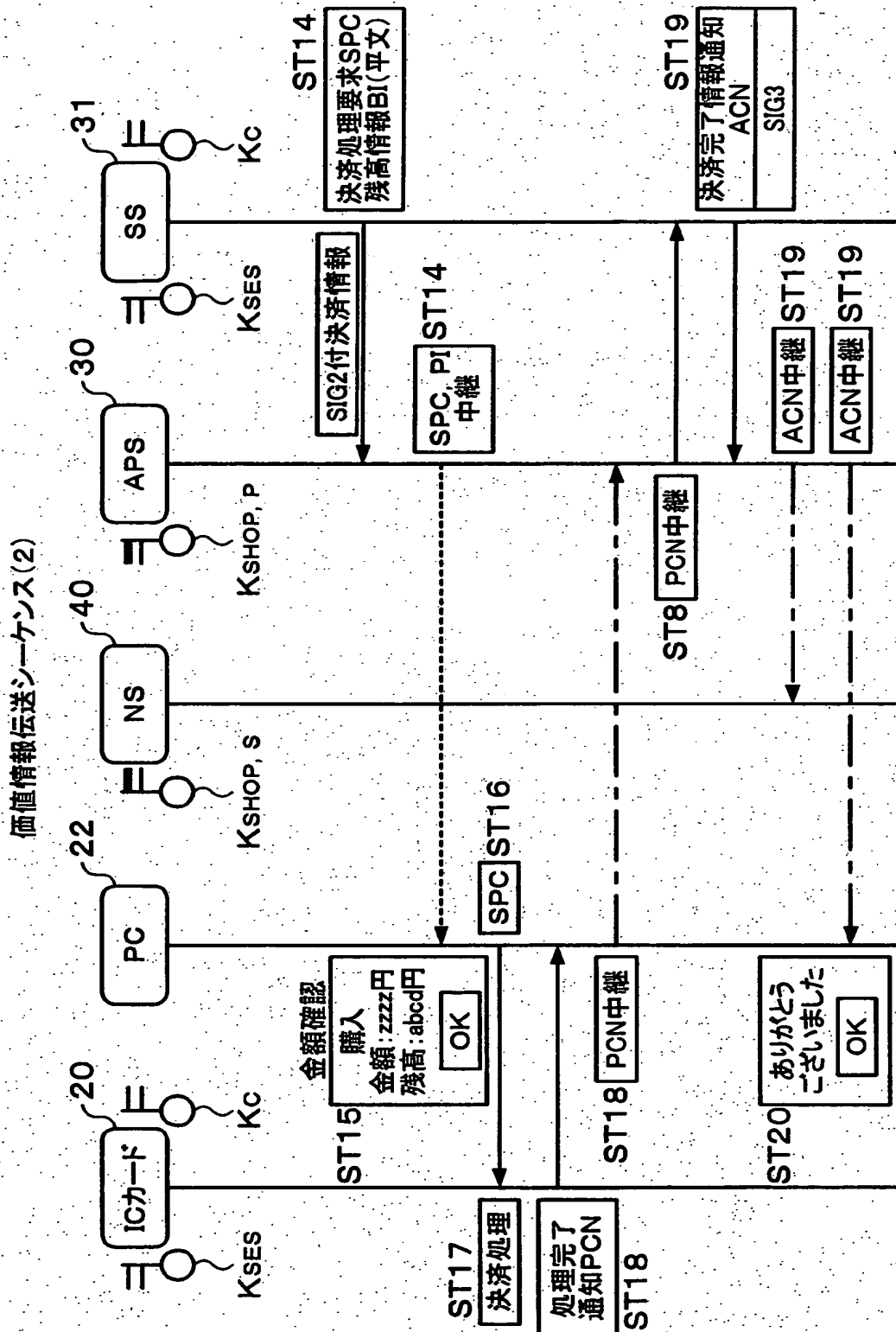
【図 9】



【図 10】



【図 11】



【図 1 2】

加盟店ページ
＜商品選択＞
商品を選択してください

品名	単価
<input checked="" type="checkbox"/> AAAA	350
<input checked="" type="checkbox"/> BBBB	400
<input type="checkbox"/> CCCC	200

購入

【図 1 3】

加盟店ページ
＜カート表示＞

品名	単価
AAAA	350
BBBB	400
<hr/>	
合計金額	750

合計

【図14】

加盟店ページ
＜支払方法選択＞

合計金額: ¥750円
◆支払方法◆

- ☐ クレジットカード
- ☐ デビットカード
- ☒ 電子マネー
- ☐ コンビニ収納代行

OK

【図15】

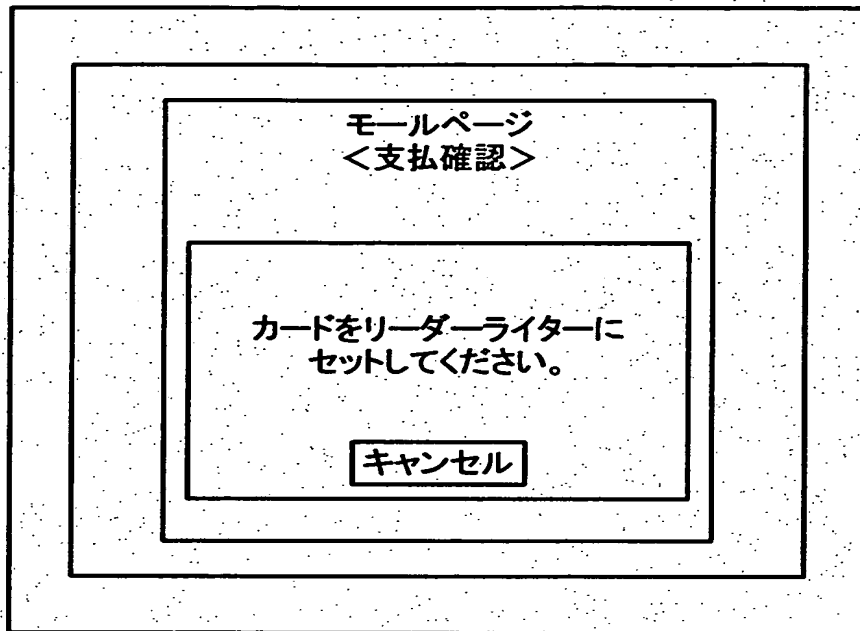
モールページ
＜支払＞

合計金額 ¥750
支払方法 電子マネー
受注番号 123456789

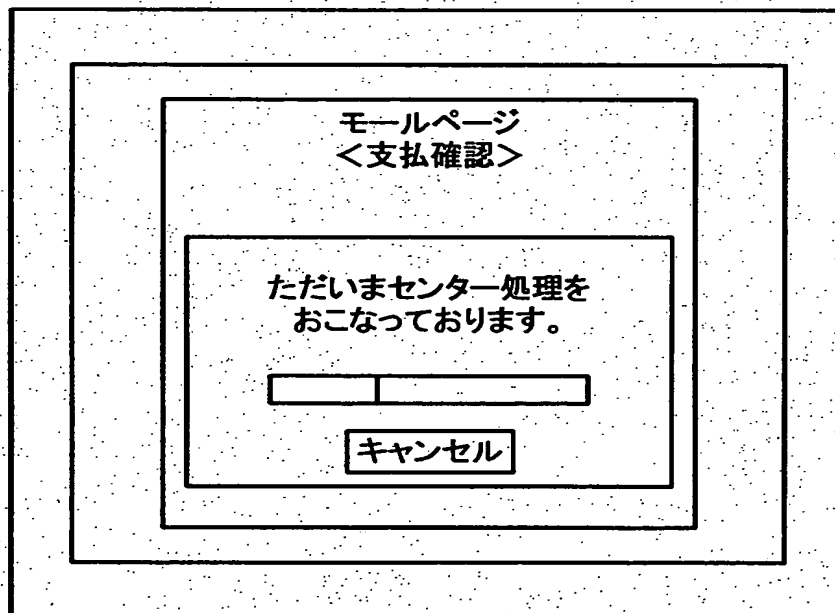
決済処理をおこないます。
よろしいですか？

OK

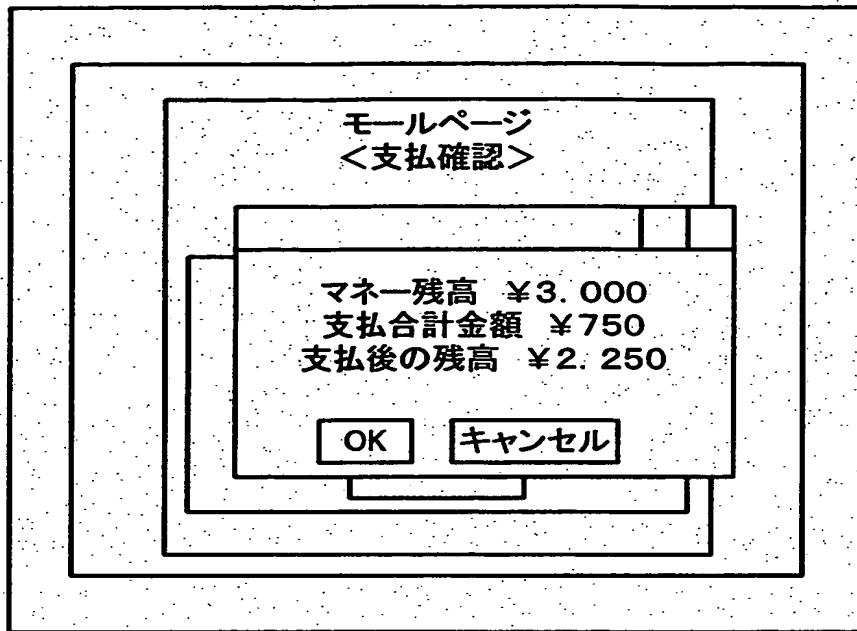
【図16】



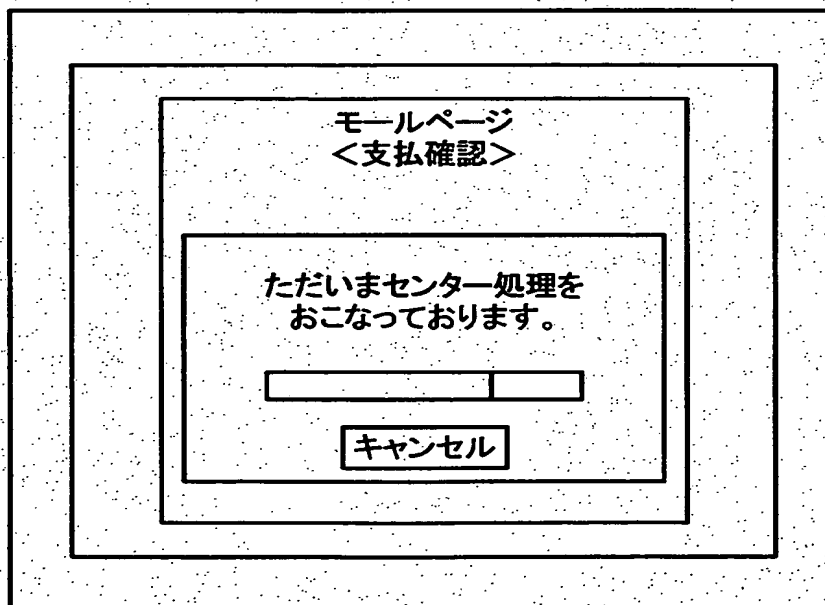
【図17】



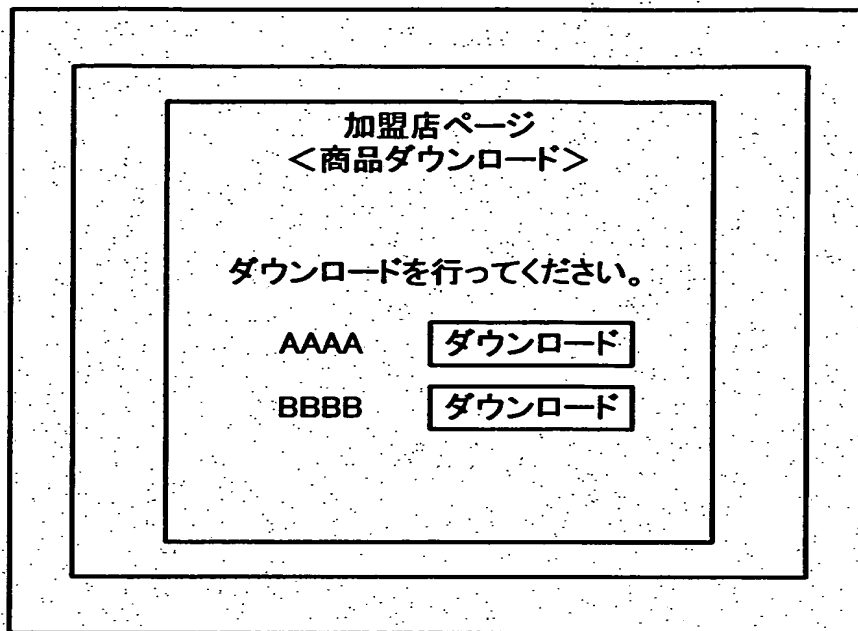
【図18】



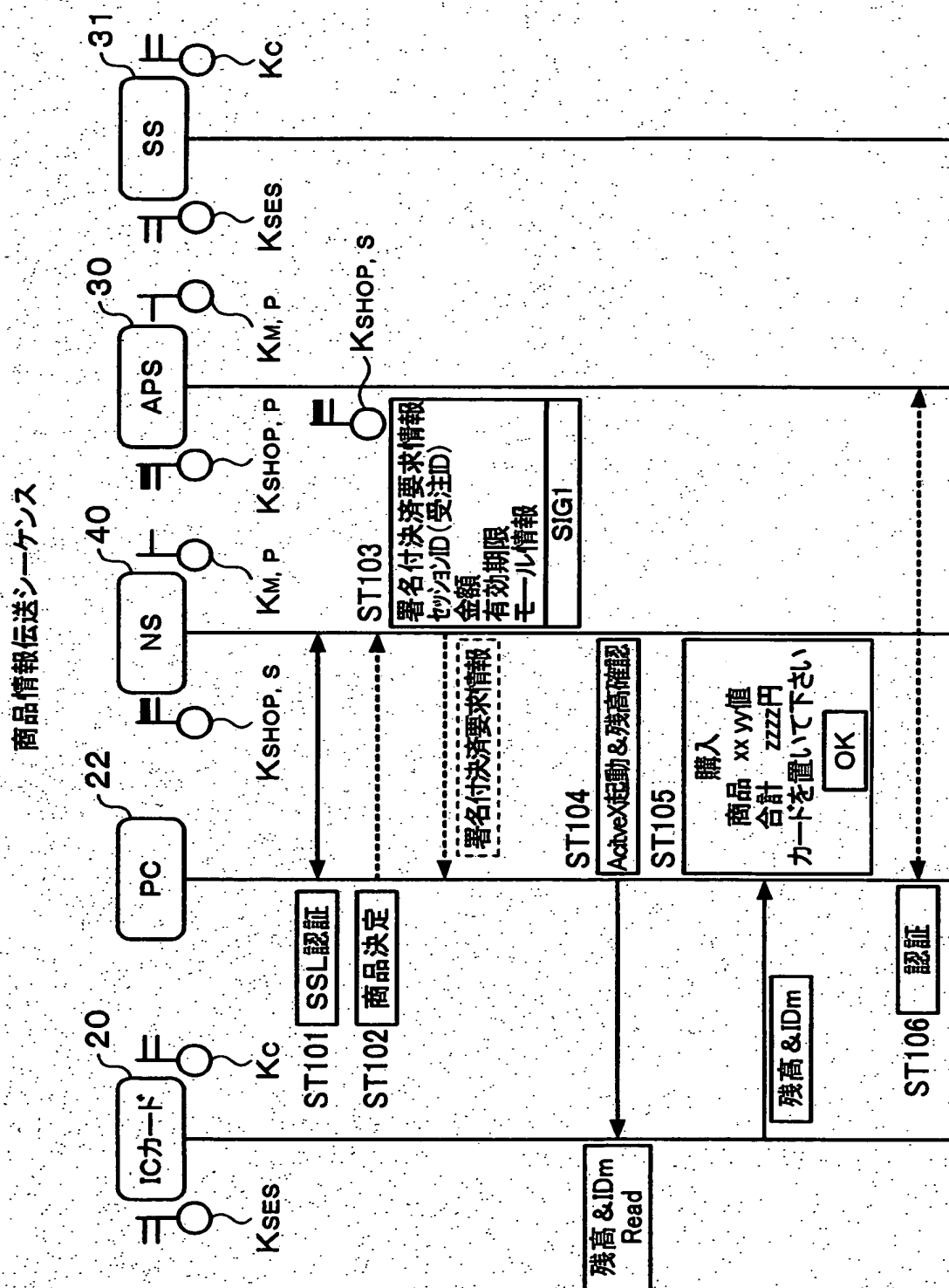
【図19】



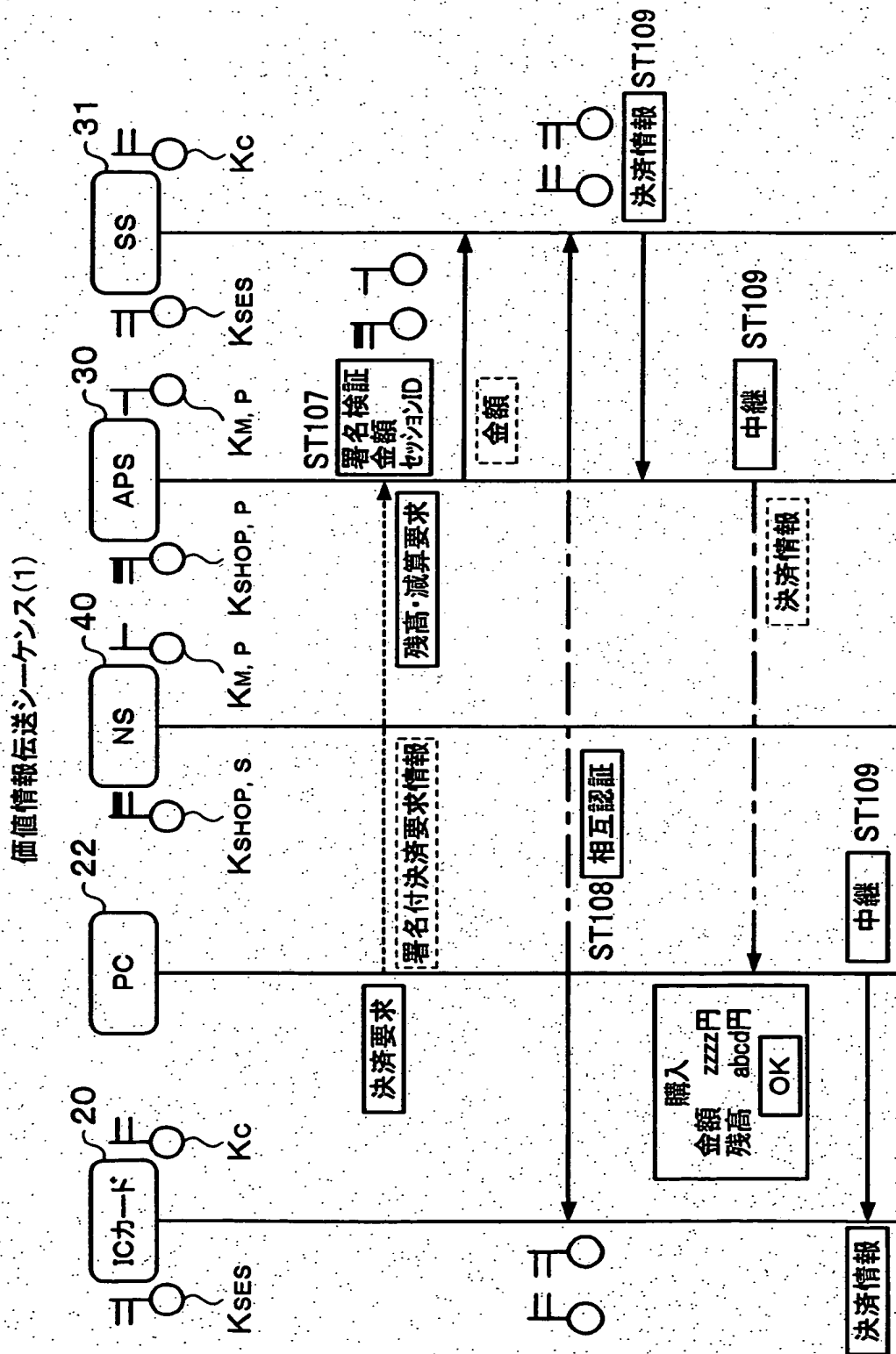
【図 20】



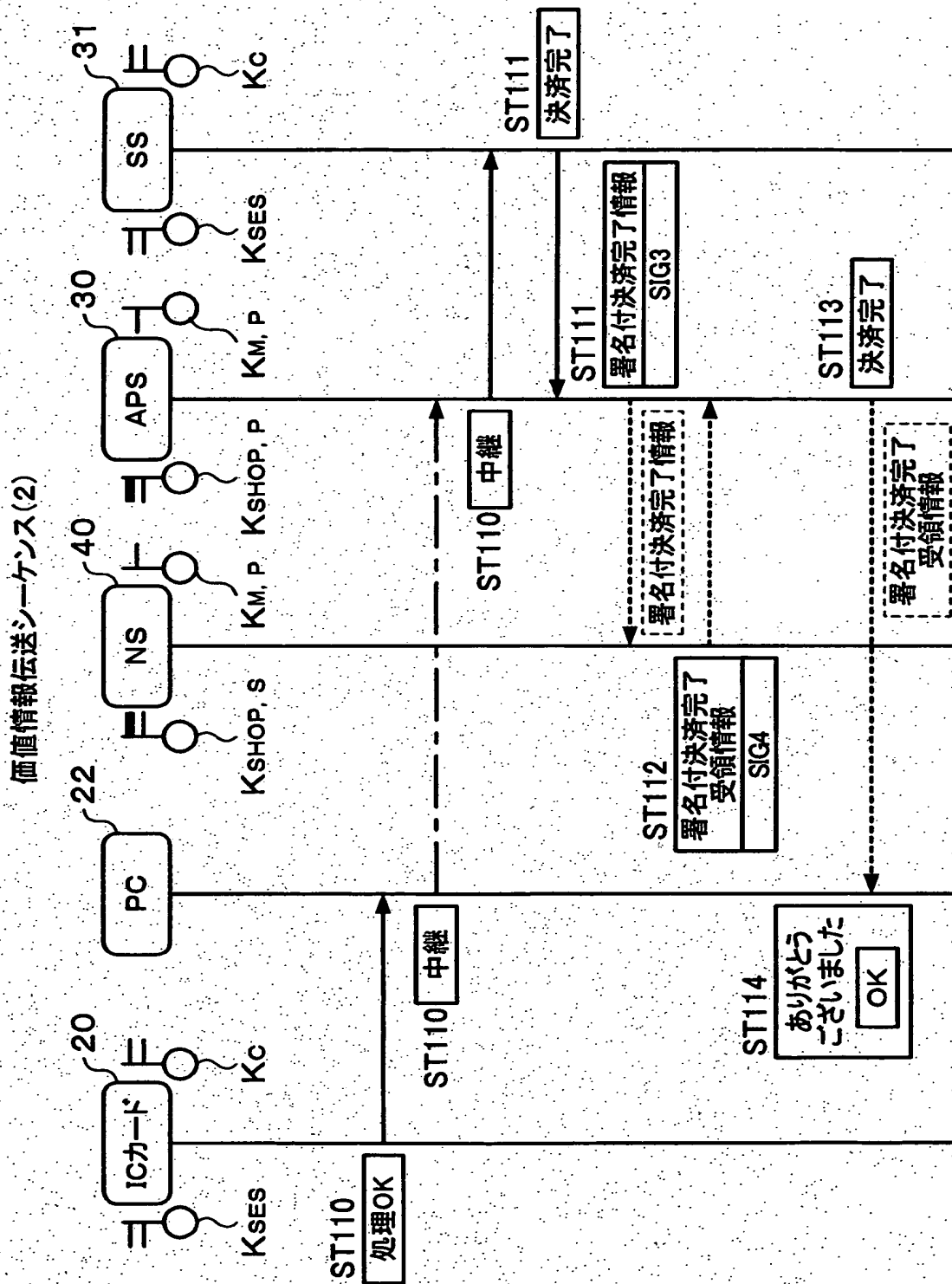
【图 2 1】



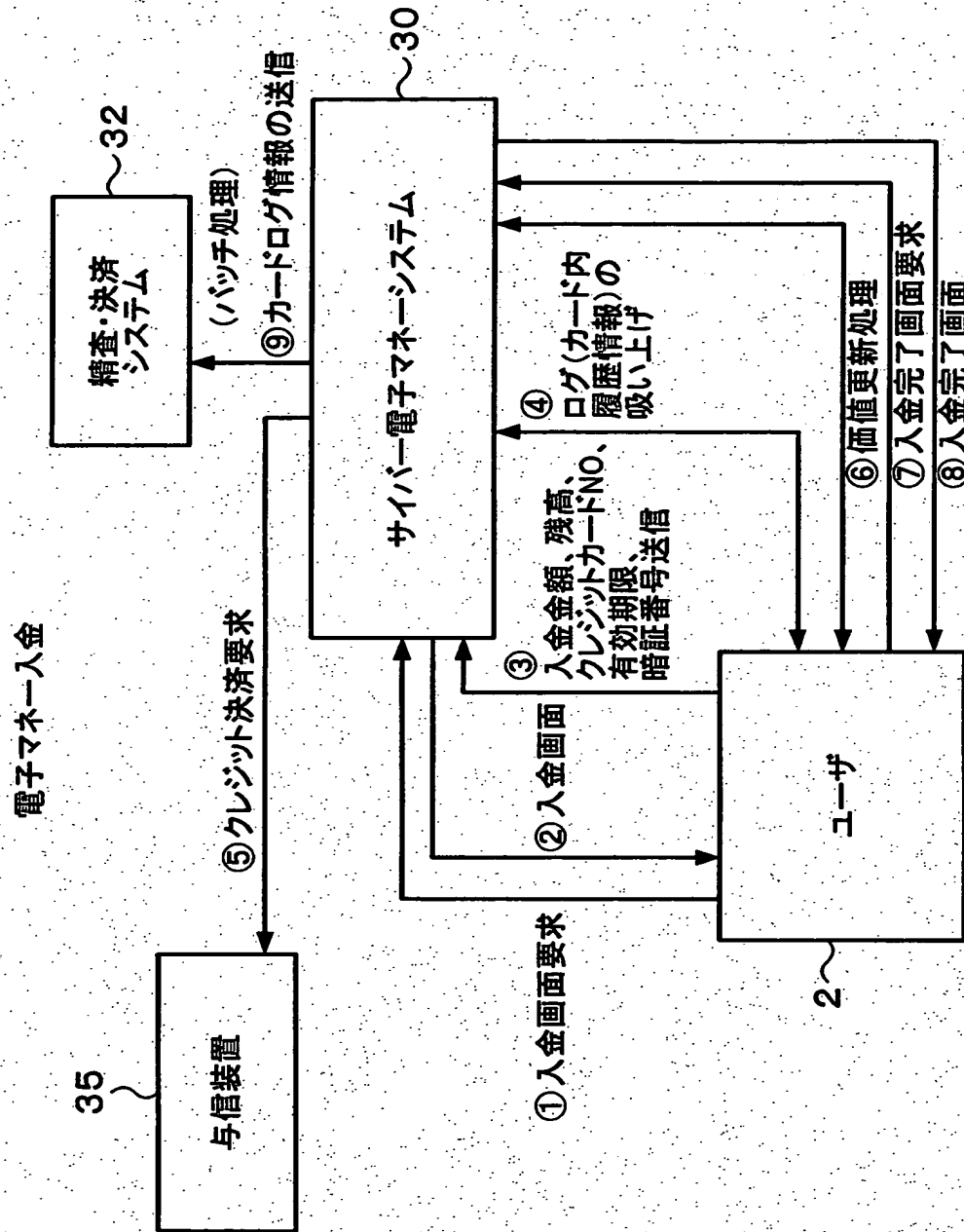
【图 2 2】



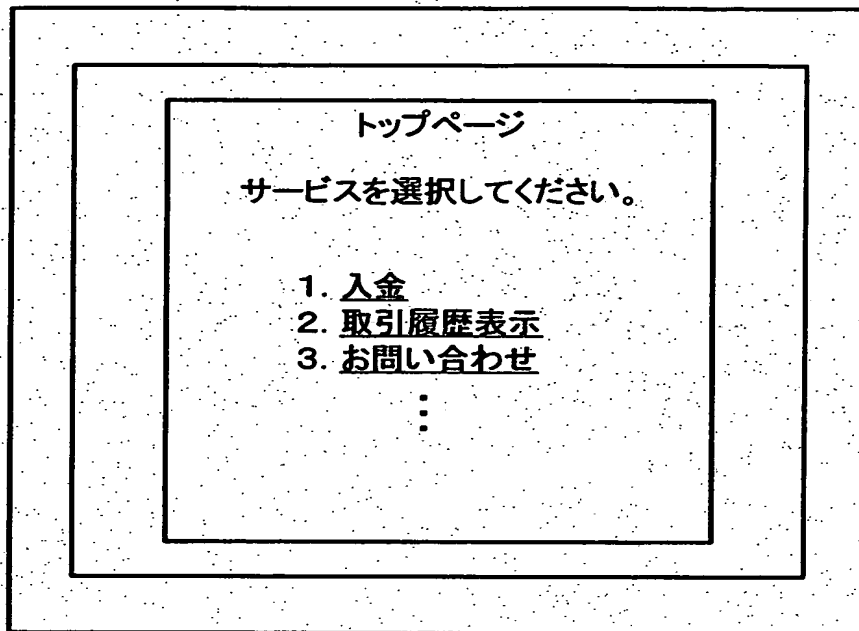
【図 23】



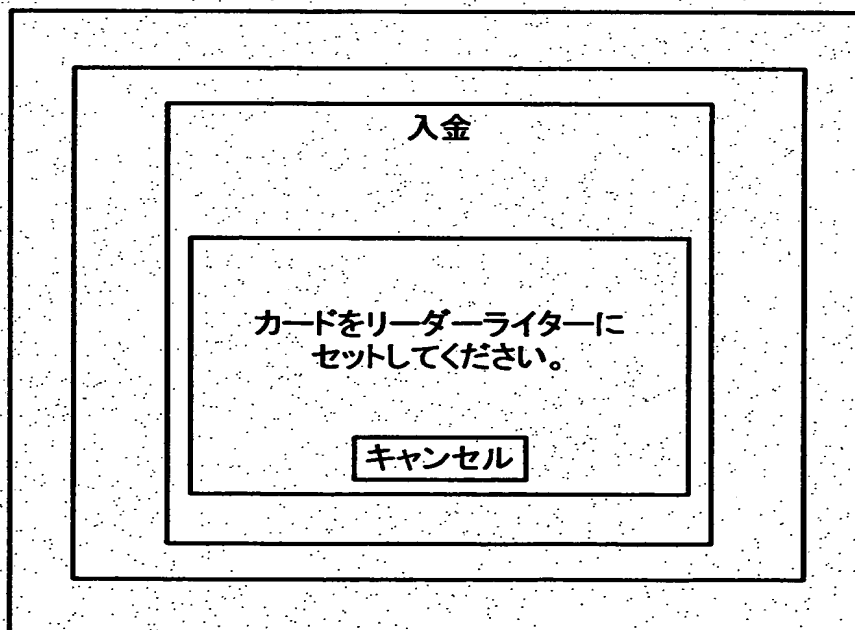
【図 24】



【図 2 5】



【図 2 6】



【図 27】

入金

ただいまセンター処理をおこなっております。

キャンセル

【図 28】

入金

マネー残高 ¥3.000

入金金額

生月日 月日

OK キャンセル

【図 29】

入金

マネー残高 ¥3.000
入金金額 ¥10.000
生月日 **月**日

OK キャンセル

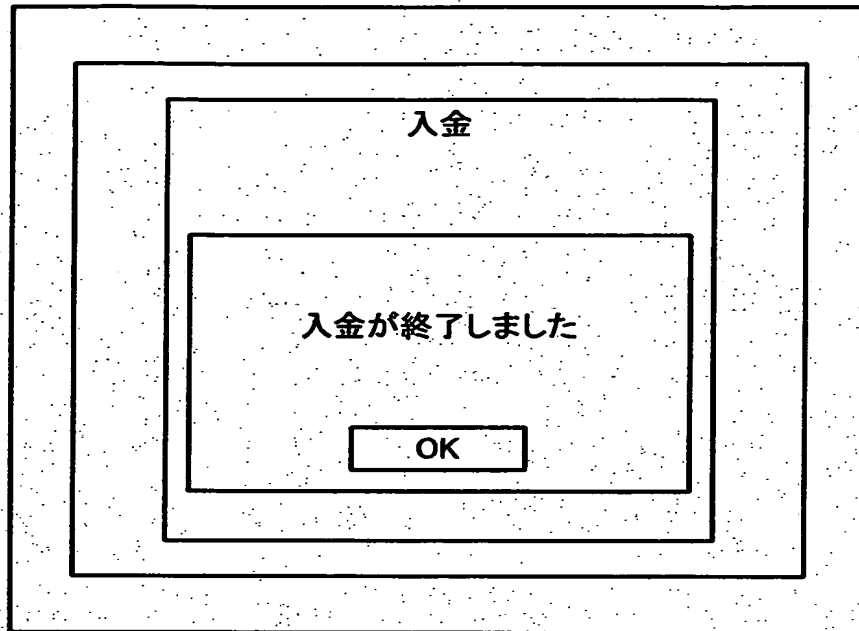
【図 30】

入金

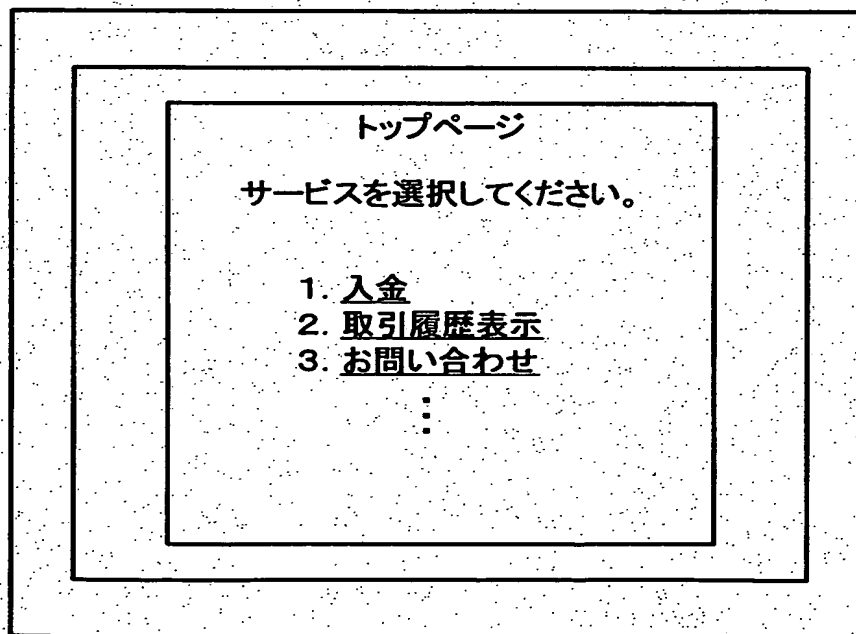
ただいまセンター処理をおこなっております。

キャンセル

【図31】



【図32】



【書類名】 要約書

【要約】

【課題】 検証回数が少なく効率的な電子決算システムを提供する。

【手段】 電子決算システムは、価値情報が記憶されたＩＣカード２０と、ＩＣカードに対する情報入出力機能を備えたクライアント装置２２と、商品またはサービスを提供する店舗装置４と、ＩＣカードと店舗装置間の決済を管理する決済管理装置３と、クライアント装置と店舗装置と決済管理装置とを双方向通信可能に接続する通信系５とから構成される。決済管理装置は、ＩＣカードで決済を行うための決済情報を、店舗装置からの決済要求情報に基づいて生成し、決済情報を決済管理装置とＩＣカードとの間で共用される共通鍵を用いて暗号化し、この暗号化された決済情報をクライアント装置に送信し、クライアント装置は、決済管理装置から受信した決済情報をＩＣカードに出力することができる。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願2001-048916
受付番号	50100258283
書類名	特許願
担当官	第七担当上席 0096
作成日	平成13年 2月28日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川6丁目7番35号
【氏名又は名称】	ソニー株式会社

【代理人】

申請人	
【識別番号】	100095957
【住所又は居所】	東京都新宿区住吉町1-12 新宿曙橋ビル は づき国際特許事務所
【氏名又は名称】	亀谷 美明

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社